S E V E N

Troubleshooting Internet Information Server

Chapter Syllabus

In this chapter, we will look at material covered in the Troubleshooting section of Microsoft's Implementing and Supporting Microsoft Internet Information Server 4.0 exam (70-087). Microsoft describes its objectives as:

- Resolving IIS configuration problems.
- Resolving security problems.
- Resolving resource access problems.
- Resolving Index Server query problems.
- Resolving Windows NT Server 4.0 and IIS setup problems.
- Using WebMaps to find and repair broken links.
- Resolving WWW service problems.
- Resolving FTP service problems.

MCSE 7.1 Troubleshooting Configurations

In this section, you will learn to identify and correct basic IIS configuration problems. Many such problems are related to the underlying Windows NT Server, the installation of IIS, or TCP/IP.

Hardware Configurations

The IIS will work improperly, if at all, if installed on incompatible hardware. Windows NT Server and IIS can run on either Intel-based computers or Reduced Instruction Set Chip (RISC)-based computers, such as the Digital Equipment Corp. (DEC) Alpha, so long as its minimum performance requirements are met.

To run on an Intel-based computer, Windows NT Server and IIS 4.0 requires:

- At least a 486DX processor running at 90 MHz.
- At least 50 Mbytes of hard disk space, with 120 Mbytes preferred.
- At least 32 Mbytes of RAM, with 48 Mbytes preferred.
- At least an SVGA monitor.

To run on a RISC-based computer, Windows NT Server and IIS 4.0 requires:

- A processor running at 150 MHz. or faster.
- At least 120 Mbytes of hard disk space, with 200 Mbytes preferred.
- At least 48 Mbytes of RAM, with 64 Mbytes preferred.
- At least an SVGA monitor.

Depending on the role a newly installed Windows NT Server is to play, it is better to deploy a computer originally designed as a "server" rather than one designed to be a "desktop" computer. Server computers often have hardware that is specially configured for higher hard disk and network throughput, and which permits the addition of a larger number of peripherals and upgrades.

Also note that whatever equipment is purchased or redeployed should be listed on the current *Windows NT Server Hardware Compatibility List*. A hard copy of this document comes with the Windows NT Server installation CD-ROM. You might also be able to find a more up-to-date version on Microsoft's Web site, as shown in Figure 7.1.

If the hard drive onto which you plan to install IIS uses the FAT format, you might consider converting it to the NTFS format. FAT provides security at the directory level, but NTFS provides security at the directory *and* file level, as previously described.

Figure 7.1 *The Hardware Compatibility List Online.*

Software Configurations

The IIS will not function properly if the underlying Windows NT Server operating system is not configured properly. It is therefore important to be sure that both Windows NT Server and the most current Service Packs have been properly installed and configured before you begin to troubleshoot the components of the Windows NT Option Pack 4.0.

WINDOWS NT SERVER 4.0

Although your Windows NT server might boot correctly, it may still not work properly because of configuration problems, such as device driver conflicts or SCSI errors. These types of problems can be identified using Windows NT's built-in utilities: Event Viewer, Windows NT Diagnostics, and Recovery.

USING EVENT VIEWER • If the server boots successfully, but not all services or components work properly, the first step in the troubleshooting process is to consult the Event Viewer application, found in the Administrative Tools pro-

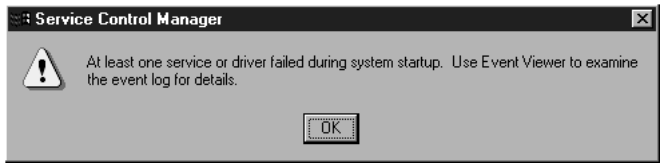

Figure 7.2 *Typical Windows NT Error Message.*

gram group. Indeed, Windows NT will often tell you to do just that with a message such as the one shown in Figure 7.2.

All critical messages are stored in the *system log*, accessed by selecting the System command under Event Viewer's View menu (see Figure 7.3).

Three kinds of events are tracked in the system log.

- **Errors.** Indicated with red stop sign symbols, these denote the failure of a Windows NT component or device.
- **Warnings.** Indicated with yellow exclamation point symbols, these denote an impending problem.
- **Information.** Indicated with blue "I" symbols, these denote a significant, but not problematic, event.

Resource access problems are noted in the *security log*. In order to use the security log, you must enable auditing via the User Manager for Domains application. This can be done using the Auditing option under User Manager for Domain's Policy menu to open the Audit Policy dialog box, as is shown in Figure 7.4.

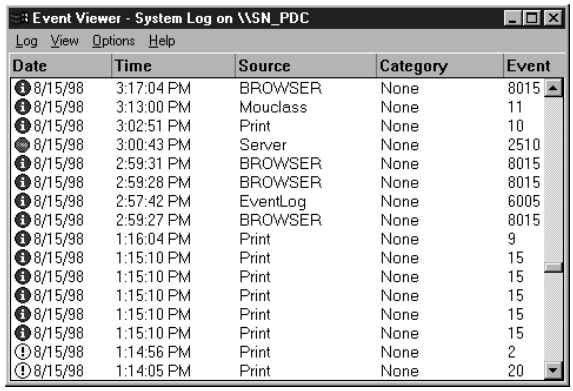

Figure 7.3 *System Log in Event Viewer.*

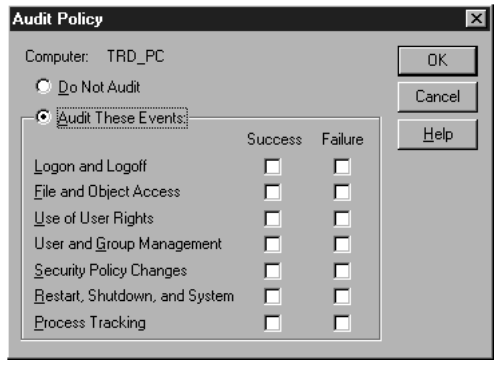

Figure 7.4 *Audit Policy Dialog Box.*

Once auditing is enabled, two types of events are tracked in the security log. These events are:

- **Success.** Indicated with a key symbol, this denotes successful resource access.
- **Failure.** Indicated with a padlock symbol, this denotes unsuccessful security access.

The *application log* collects messages from native Windows NT (WIN32) applications, such as those of the IIS. Log files can grow to 512 Kbytes in size, by default. Their events are overwritten after seven days. For more extensive logging intervals, you can change this behavior in the Event Log Settings dialog box, accessed via the Log Settings command under the Log menu as shown in Figure 7.5.

The system log is most useful for isolating problems such as those that generate the message shown in Figure 7.2. To examine an event, double-click

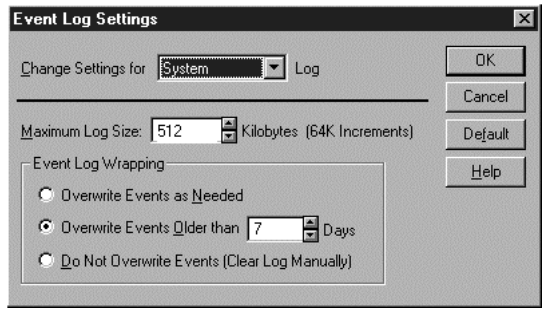

Figure 7.5 *Log Settings Dialog Box.*

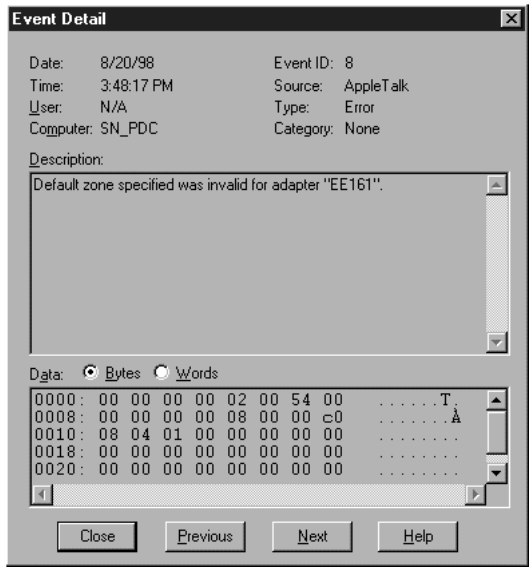

Figure 7.6 *Event Detail Dialog Box.*

on it in the log window to open the Event Detail dialog box, as is shown in Figure 7.6.

The information listed here includes:

- Date
- Time
- User account (if applicable)
- Computer
- Event identifier
- Source component
- Event type
- Event category
- Description
- Data dump (in hexadecimal format)

From this data you will either be able to determine what the problem is (e.g., you have too little disk space) or what to ask Microsoft technical support (e.g., "what does Event ID 8 mean?").

USING WINDOWS NT DIAGNOSTICS • Windows NT Diagnostics provides detailed system configuration reports, as shown in Figure 7.7. This can help you determine if problems are a result of IIS operations or if they originate in the operating system.

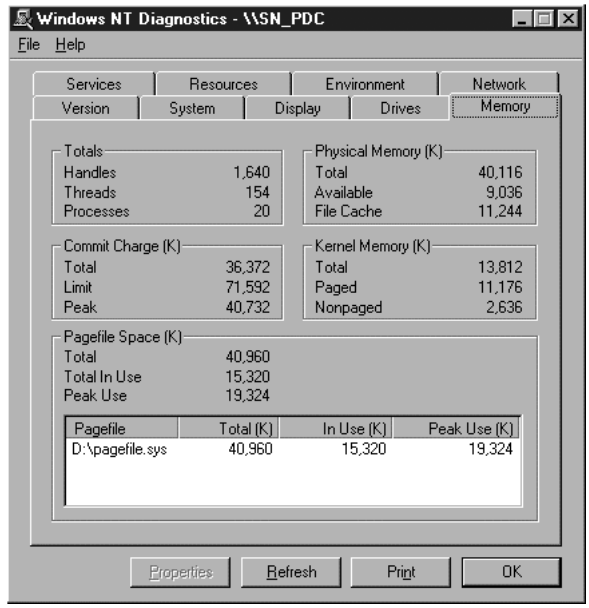

Figure 7.7 *Windows NT Diagnostics Dialog Box.*

Here displayed is information from the HKEY_LOCAL_MACHINE Registry tree. The dialog box contains tabs for the following:

- **Version**. Lists the current version, build number, Service Pack update, and registered owner.
- **System**. Contains CPU and hardware information.
- **Display**. Contains video adapter information.
- **Drives**. Lists all drives and drive types, as well as attached network drives.
- **Memory**. Contains current physical RAM and Virtual Memory information.
- **Services**. Lists services and their status.
- **Resources**. Lists devices information, detailed by port number, interrupt, DMA channel and UMB location.
- **Environment**. Contains environment variables for command prompt sessions, such as \WINNT directory location and "temp" directory locations.
- **Network**. Lists network components and their status.

USING RECOVERY • The Recovery utility can be configured under the Startup/Shutdown tab of the System control panel, as shown in Figure 7.8.

Here you can enable settings to choose the operating system that will boot by default and establish how long the server will pause so that you can make another choice. You can also enable options to write event data to the system log, alert an administrator of problems, or automatically reboot the system if the server freezes (e.g., stops all processes). Enabling the Write debugging information to check box creates a *dump file* that you can analyze yourself or in conjunction with Microsoft technical support. With the option configured, the data that was in memory at the time a stop error occurred is written to the paging file on the boot partition. When the computer is restarted, the data in the paging file is then saved to a dump file.

In order for this to work, there must be a paging file on the boot partition that is larger than the amount of physical RAM installed in the server. In addition, there must be enough hard drive space on the disk drive to which the dump file will be saved to accomodate a file the same size as the server's physical RAM.

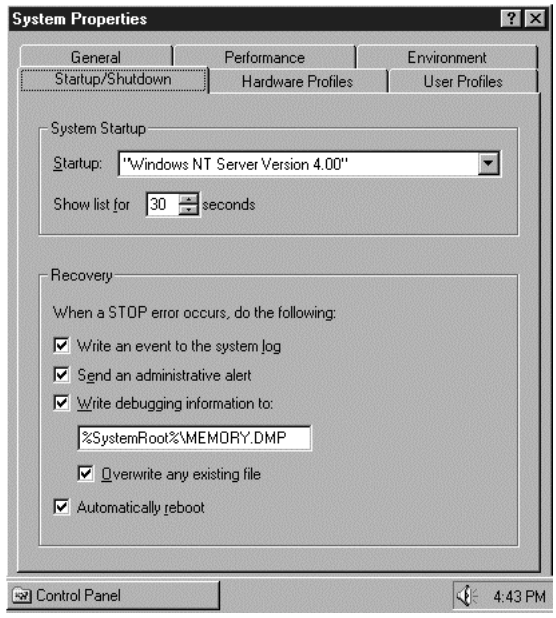

Figure 7.8 *Startup/Shutdown Tab in the System Control Panel.*

SERVICE PACKS

Along with Windows NT Option Pack 4.0, you need to install the latest Windows NT Service Pack. This is a free Microsoft update that contains bug fixes and improvements made to Windows NT Server since it shipped originally. It can be downloaded from the Microsoft Web site (as shown in Figure 7.9) or ordered on CD-ROM. (Visit the main Microsoft Web site to find the newest location for Service Packs.)

The minimum requirement for the Windows NT Option Pack 4.0 is Service Pack 3. If you install Service Pack 4, the software will detect that at least one of the operating system components contain a known year 2000 (Y2K) issue. For example, you might be admonished to update your system to Internet Explorer 4.01 Service Pack 1, Data Access Components 2.0 Service Pack 1, or Site Server Express 3.0. Such components can be upgraded individually from the Service Pack 4 compact disc, or downloaded from the URL http://support.microsoft.com/support/downloads/.

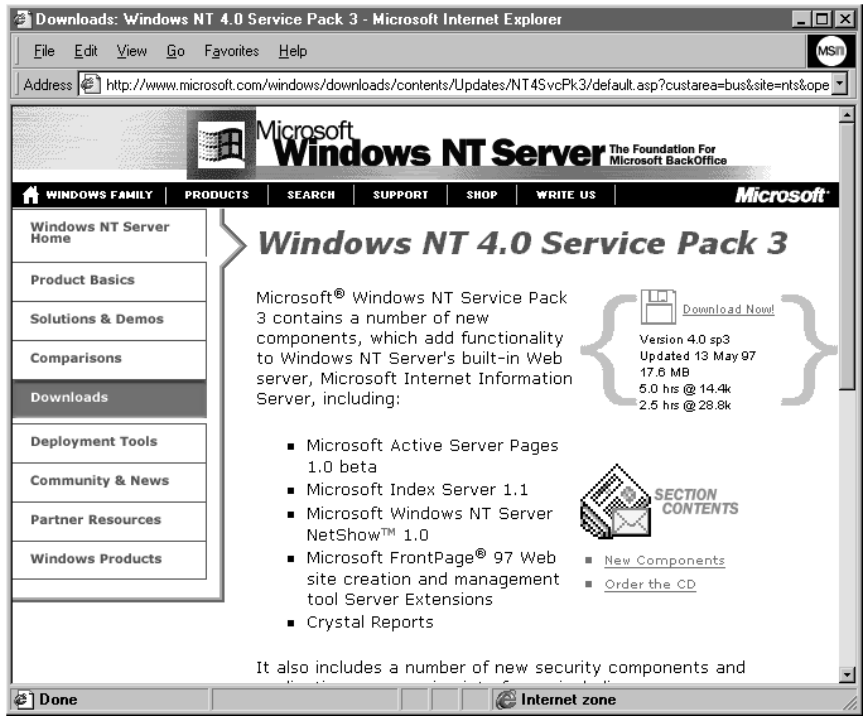

Figure 7.9 *Downloading Windows NT Service Pack.*

Issues relating to the installation of the Windows NT Option Pack 4.0 and its components will be discussed in the following sections.

Network Configurations

Another opportunity for IIS problems resides with the network configuration. You must configure your server with a static IP address (rather than permitting a DHCP server to assign it dynamically). IP addresses are generally obtained from an ISP or some authority within your organization. If these are configured incorrectly, communications problems will result.

USING THE NETWORK CONTROL PANEL

Network protocols and their associated hardware bindings are configured in the Network application, found in the Control Panel program group. Its interface contains five tabs whose contents should be verified when problems occur.

IDENTIFICATION TAB • As shown in Figure 7.10, here is where the computer's NetBIOS name and the name of the workgroup or domain it is a member of is configured.

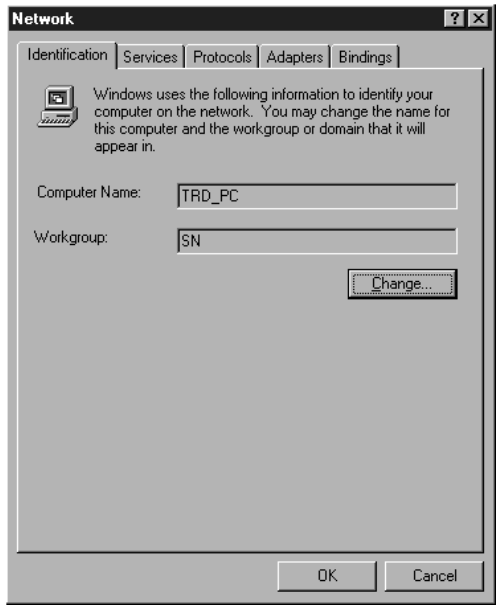

Figure 7.10 *The Identification Tab.*

SERVICES TAB • As shown in Figure 7.11, here is where network services are added, removed, and configured.

Besides those shown in Figure 7.11, other relevant Windows NT network services include DHCP Relay Agent, DHCP Server, DNS Server, TCP/IP Printing, Remote Access Services, Router Information Protocol (RIP) for Internet Protocol, and WINS server.

ADAPTERS TAB • As shown in Figure 7.12, here is where network adapter hardware is added, removed, and configured.

Windows NT Servers can have multiple network adapters for different media types or for joining different network segments when acting as a router.

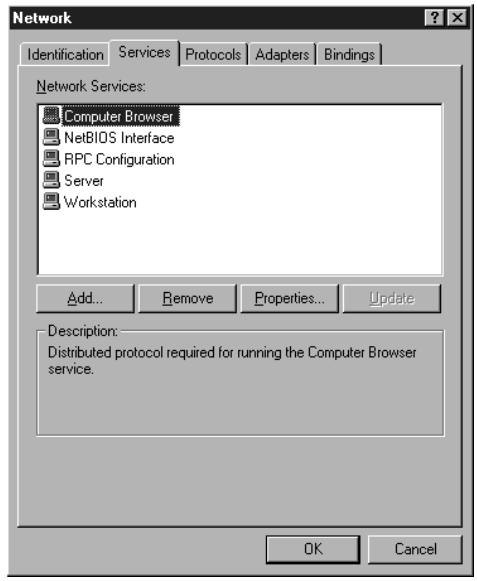

Figure 7.11 *The Services Tab.*

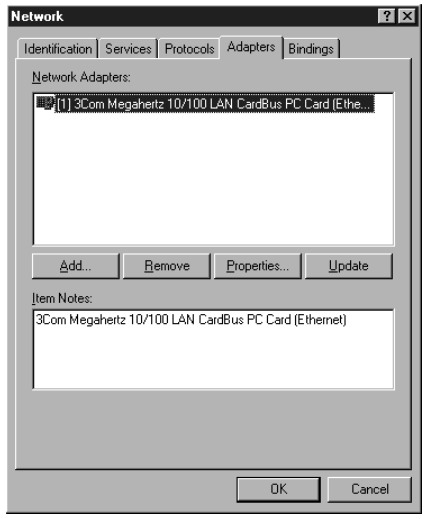

Figure 7.12 *The Adapters Tab.*

Pressing the Properties button provides access to a network adapter's three main settings.

- **IRQ**. The IRQ, or *Interrupt Request*, refers to when the CPU will process the data in the network adapter's buffer. IRQ's can also be set through hardware switches on the network adapter or via a manufacturer's configuration software.
- **I/O address**. The I/O, or *Input/Output address,* pertains to the network adapter's unique logical location within the system. It is to this address that device instructions are sent.
- **Transceiver type**. The transceiver type is associated with the cabling used on your network. It ensures that signals are properly transmitted and received across the medium.

BINDINGS TAB • As shown in Figure 7.13, here is where network bindings are added, removed, and configured. Bindings act as the interfaces between network hardware, protocols, and services.

Here you can change the associations of services and network hardware with the various protocols. Use the Show Binding for pop-up menu to switch between views for network adapters, services, and protocols. The Enable button activates a binding. The Disable button de-activates it. The Move Up and Move Down buttons permit you to rearrange the order in which the bindings are applied.

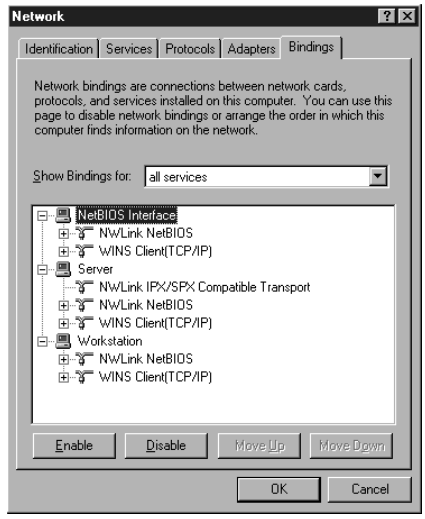

Figure 7.13 *The Bindings Tab.*

PROTOCOLS TAB • As shown in Figure 7.14, here is where network protocols such as TCP/IP are added, removed, and configured.

To configure TCP/IP, select TCP/IP Protocol under the Protocols tab and press the Properties button. This will open the window that is shown in

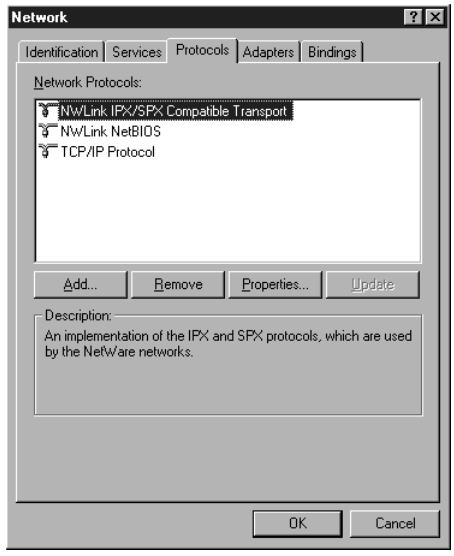

Figure 7.14 *The Protocols Tab.*

Figure 7.15, which contains IP Address, DNS, WINS Address, DHCP Relay and Routing tabs.

Because this is a server computer, you will need to select the Specify an IP address radio button. You must then enter the correct IP address, subnet mask, and gateway address.

The association of domain names with machine addresses is handled by Domain Name System (DNS) servers. Enter the machine addresses for your network's DNS servers in DNS Service Search Order field, in order of preference. Enter the domain(s) for your network in the Domain Suffix Search Order field (as shown in Figure 7.16).

Windows NT Server can also act as a DNS server itself.

The Windows Internet Name Service (WINS) is somewhat like DNS, except that it maps IP addresses to NetBIOS names instead of domain names. Configure the IP addresses of the Windows NT servers that are running WINS for your network in the Primary WINS Server and Secondary WINS Server fields under the WINS Address tab (as shown in Figure 7.17).

By default, the Enable LMHOSTS Lookup checkbox is selected. This permits the use of a text list of IP address-to-NetBIOS name mappings for computers outside the local subnet. If the Enable DNS for Windows Resolution checkbox is selected, Windows NT will lookup NetBIOS names against a DNS server.

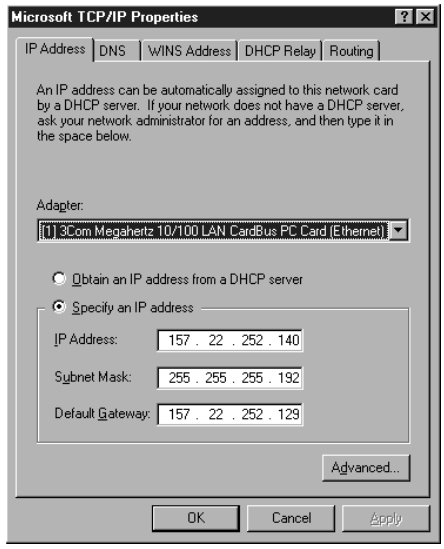

Figure 7.15 *Configuring TCP/IP.*

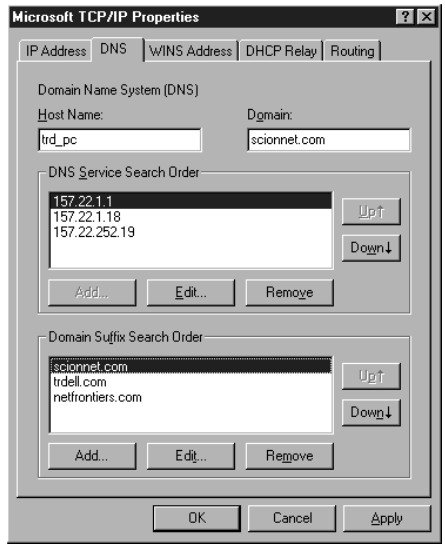

Figure 7.16 *Configuring DNS Settings.*

The DHCP Relay service permits broadcast messages from BOOTP and DHCP servers to reach clients over routers. This is useful on networks with routers that do not permit the transfer of such broadcasts.

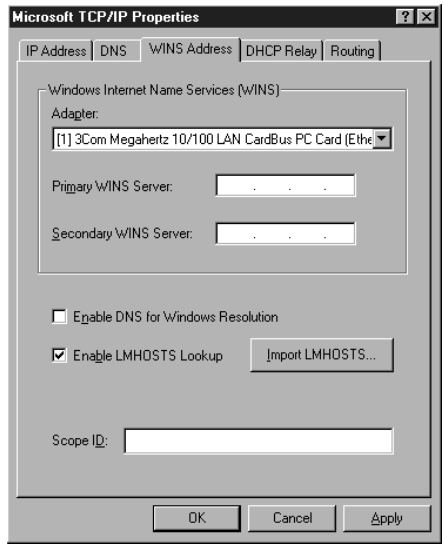

Figure 7.17 *Configuring WINS.*

The use of NetBIOS *scopes* permit the creation of logical TCP/IP networks that are invisible to one another. If your network is configured in this manner, you will need to configure the Scope ID field to be able to communicate with other hosts in your scope.

It is possible for a Windows NT server to reside on more than one network at the same time, a situation referred to as *multi-homing*. Enabling the Enable IP Forwarding checkbox under the Routing tab will allow packets to move between these networks.

SOLVING TCP/IP CONFIGURATION PROBLEMS

If you fail to properly configure the previously mentioned dialog boxes, a number of errors are possible.

IP ADDRESS PROBLEMS • It is important that the IP address used by the IIS computer is properly mapped to the correct host name in your network's DNS database or LMHOSTS file. If not, Web browsers and other clients will only be able to access the IIS by referring to an explicit IP address. For example, imagine a server with the host name "www.scionnet.com" and an IP address of 157.22.252.100. If you change the IP address to 157.22.252.101, the server will still be able to communicate using the number, but the host name would no longer be resolved to the correct computer. Because of this, you must be sure to use the exact IP address given to you by whoever is responsible for the network's DNS, an administrator or your ISP.

As previously described, part of each IP address specifies the network and part specifies the host. When subnetting is used, part of the host address is used to specify the subnet. Because of this, mistyping the IP address can cause different problems based on the octet(s) that are incorrect.

For example, if you mistyped 157.22.252.100 as 175.22.252.100, the server would be identified with an entirely different network. If the server (e.g., 175.22.252.100) attempts to send a message to a local client (e.g., 157.22.252.105), it will not go through because the server thinks the client address is on a remote network.

If the client (e.g., 157.22.252.105) attempts to send a message to the local server at the mistyped address (e.g., 175.22.252.100), the server will be seen as remote and the packets will be routed through the default gateway. If the client (e.g., 157.22.252.105) attempts to send a message to the local server at the correct address (e.g., 157.22.252.100), the packets will stay on the local

network, but there will be no server at that address to receive them. Either way, the messages will not go through.

SUBNET MASK PROBLEMS • If the IP address is configured correctly, but the wrong subnet mask is used, problems will also occur. For example, the server could be configured with the address 157.22.252.100 and the subnet mask 255.255.255.0. In this case, 157.22.252 denotes the network and 100 denotes the host. Suppose, however, that the network had actually been divided into two subnets using the subnet mask 255.255.255.128. All host addresses would then be distributed between two subnets, 1-126 and 129-254. In this case, a client with an IP address of 157.22.252.130 would be able to communicate with the server. The subnet mask is only used in routing outgoing messages, so the difference in subnet masks would not affect incoming communications. The server would not be able to communicate with the client, however, because the incorrect subnet mask would indicate that the client is local when it is actually remote.

Table 7.1 provides a review of some typical small-network subnet configurations.

Table 7.1 *Class C Subnets*[*]

Subnet Mask	Segments	Host Ranges*
255.255.255.0	1	1-254
255.255.255.128	2	1-126, 129-254
255.255.255.192	4	1-62, 65-126, 129-190, 193-254
255.255.255.224	8	1-30, 33-62, 65-94, 97-126, 129-158, 161-190, 193-222, 225-254
255.255.255.240	16	1-14, 17-30, 33-46, 49-62, 65-78, 81-94, 97-110, 113-126, 129-142, 145-158, 161-174, 177-190, 193-206, 209-222, 225-238, 241-254
255.255.255.248	32	1-6, etc.

[*] first and last address in the range is reserved.

In short, mistakes in the subnet mask configuration cause some packets to be routed when they should be kept local and some packets to remain local when they should be routed. Such mistakes manifest themselves as intermittent connections.

GATEWAY ADDRESS PROBLEMS • Mistyping the default gateway (router) address causes problems similar to those caused by a misconfigured subnet mask. Because the router is only responsible for routing packets to remote networks, communications between a client and the incorrectly configured server on the same subnet can still take place. Likewise, a remote client can

also send packets to the server. The server will not be able to send packets to the remote client, however.

Typically, the first or last non-reserved IP address in a given range is used for the router address. Where the network is divided into two subnets with the subnet mask 255.255.255.128, for example, all host addresses are then distributed between two subnets, 1–126 and 129–254. The gateway addresses might be x.x.x.1 and x.x.x.129 or x.x.x.126 and x.x.x.254, respectively.

DHCP Address Problems • By using the Dynamic Host Configuration Protocol (DHCP), administrators can avoid the effort of configuring static IP addresses on clients by letting workstations obtain their addresses dynamically. The DHCP server manages a range of available addresses that it doles out automatically when a workstation attempts to use a TCP/IP service. These addresses are *leased* for a limited time.

Windows NT includes the DHCP Server service, which is installed as a network service (via the Network Control Panel application). Once installed, it can be configured using the DHCP Manager application found in the Administrative Tools program group (see Figure 7.18).

The part of your network's IP address range that you wish to share dynamically is called its *scope*. To assign dynamic addresses, choose the Create command under the Scope menu to open the Create Scope dialog box, as shown in Figure 7.19.

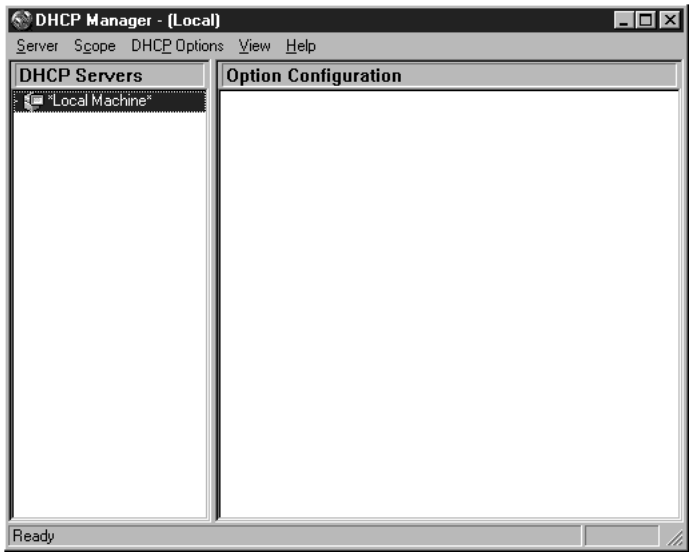

Figure 7.18 *DHCP Manager.*

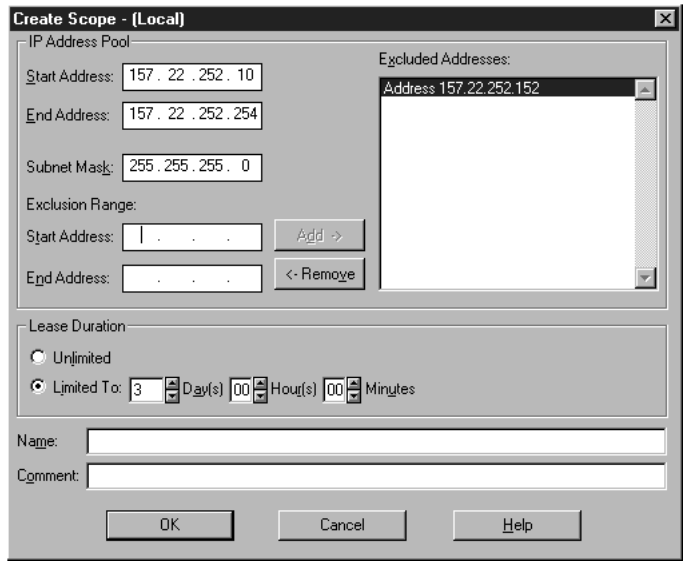

Figure 7.19 *Create Scope Dialog Box.*

The first and last IP addresses in the range are entered here, along with the subnet mask. If there are any addresses that fall within the range which you do not want treated dynamically, you may add them to the Excluded Addresses list. Finally, you may set the lease duration here.

When setting up the DHCP Server, you will need to make sure that the scope of addresses you have given it to administer are not already in use. Any individual addresses already assigned to hosts should be removed from the scope using the DHCP Server's exclusion list. Be especially careful not to have overlapping scopes administered from multiple DHCP servers.

In order to ensure that IP addresses are not assigned to hosts that no longer need them, each client is subject to a *lease*. This is the duration of time that each host is permitted to use an IP address before the DHCP Server reclaims it. Clients are permitted to renew their leases when 50 percent of the duration has elapsed and when 87.5 percent of the duration has elapsed, or after a restart. In setting lease values, you should adhere to the following rules:

- The lease duration should be shorter when the number of clients is near to or exceeds the number of available IP addresses.
- The lease duration should be longer when there are plenty of IP addresses to go around.

Lease durations can differ from scope to scope.

Several other parameters can also be assigned by the DHCP Server:

- **Router**. Used to include the IP address of the default gateway for the subnet.
- **DNS Server**. Used to include the IP addresses of the DNS servers on the network.
- **Domain Name**. Used to include the domain name that should be used by the host.
- **NetBIOS Scope ID**. Used when you wish to separate clients into logical network segments so that they cannot communicate with each other.
- **WINS/NBNS Servers**. Used to include the IP addresses of servers that can be used for IP address-to-NetBIOS name resolution.
- **WINS/NBT Node Type**. Used to identify the methods that will be used for IP address-to-NetBIOS name resolution.

DHCP Relay Problems • In order to obtain an IP address, workstations will send out network broadcast packets to any available BOOTP/DHCP servers. Since one function of a router is to limit broadcast traffic to its network of origin, a workstation on one side of a router will often be unable to communicate with a DHCP server on the other side. To overcome this limitation, Windows NT provides the DHCP Relay agent, which can be installed as a network service. It will pass broadcast traffic directly to the DHCP servers you designate under the DHCP Relay tab of the TCP/IP Properties dialog box (see Figure 7.20).

BOOTP, or *Bootstrap Protocol*, is an earlier UNIX technique for obtaining dynamic IP addresses. DHCP is based upon this earlier, more limited protocol. Because of this, DHCP servers can process requests from BOOTP clients as well.

Name Resolution Problems • Windows NT clients use two name resolution methodologies when accessing the network. When native Windows NT networking is in use, NetBIOS name resolution is employed. This is supported by all Windows NT protocols, although in the case of TCP/IP, the add-on WINS service is needed. When TCP/IP-based services are in use, host name resolution is employed. This is only necessary when using intranet or Internet applications, and is made possible by DNS servers.

WINS clients automatically contact the WINS server upon startup to provide their NetBIOS Computer Names and IP addresses. This information goes into a central database maintained by the WINS server.

Clients can be configured to make the WINS server their primary method of NetBIOS name resolution under the WINS Address tab of the TCP/IP Properties dialog box (see Figure 7.17).

Host name resolution is needed when clients make use of TCP/IP-based applications such as the WWW, Gopher, FTP, Telnet, and IRC. Three components come into play during this process. When a client requests a host name-to-IP address mapping, it is acting as a domain name *resolver*. The service that receives the client's request is the domain *name server*, such as the Windows NT DNS Server. A local DNS server will know about the address mappings for the local network, but not for the rest of the world. When a client requests an address that resides on the Internet, the local DNS server must pass the request on to the *domain name space*. This refers to a distributed database of unique IP address-to-host name mappings that resides on DNS servers world wide.

Clients can be configured to use DNS servers under the DNS tab of the TCP/IP Properties dialog box (see Figure 7.16).

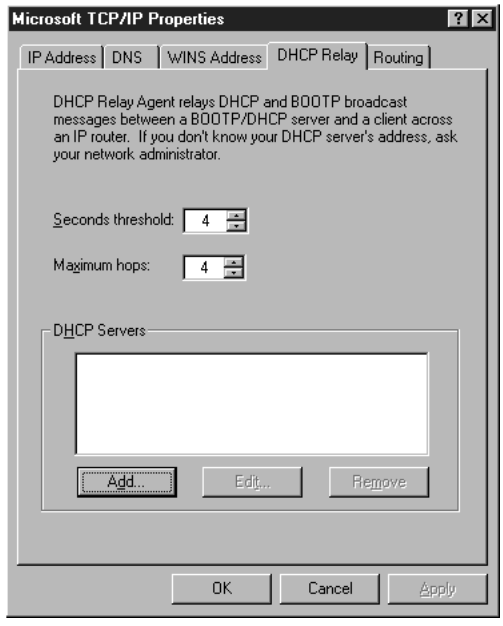

Figure 7.20 *DHCP Relay tab in the TCP/IP Properties Dialog Box.*

To determine if the local host is capable of resolving a domain name, you can use the NSLOOKUP utility. It can be launched from the Command Prompt with the following command:

```
NSLOOKUP <host_name>
```

If it works, the appropriate IP address will be returned.

Study Break

Study Break: Checking Your TCP/IP Configuration

Practice what you have learned by making sure the server's TCP/IP connectivity is working properly. One of the easiest ways to do this is simply to launch Internet Explorer and attempt to view a remote Web site. If this fails, however, you can employ some useful Windows NT utilities in troubleshooting.

IPCONFIG will tell you the TCP/IP settings with which your computer is configured. You can then review them for errors. Use the /ALL switch to see DHCP and WINS information as well.

PING will tell you if a remote host is receiving your messages. Use the IP address of a properly configured local host. If your TCP/IP configuration is working, it will respond. Then try the IP address of a remote host. If all is well with your network and router configurations, it should respond too.

TRACERT (Trace Route) will tell you how many routers are crossed as traffic moves from a local host to a remote host.

These are all DOS programs that can be launched from Command Prompt.

MCSE 7.2 Troubleshooting Security

In troubleshooting security, one is either attempting to keep people from getting access to resources that they should be restricted from, or to give people access to resources that they should have. In this section, you will learn to troubleshoot such areas as firewalls, anonymous access, user logons, network access, port numbers, NTFS permissions, and SSL connections.

Troubleshooting Firewalls

A *firewall* is software running on a server or router that can be used to filter the kinds of traffic that is allowed to pass between your network and the

Internet. For example, you might permit HTTP traffic to move through the firewall, but prohibit FTP traffic. Firewalls can also be used to filter and block traffic originating from networks or hosts known to be insecure.

If users cannot gain access to IIS resources from the Internet (assuming you want them to), check to see that the firewall is configured to allow such access. In some cases, your network's firewall might be so restrictive that traffic is not permitted to pass between the IIS and the outside world. If such access is desired, you might consider moving the IIS outside the network and beyond the firewall.

Troubleshooting Anonymous Access

Anonymous access is a method of permitting unknown users to access your Web or FTP server directories. Typically, such users supply the user ID *anonymous* and, as a courtesy, their email addresses as passwords. Under IIS, the *IUSR_<server_name>* account is used to permit this type of access. As shown in Figure 7.21, you can establish anonymous user permissions for this account using Windows NT Server's User Manager for Domains application.

If the IUSR account (or whichever account you might have reconfigured for this purpose) is disabled or deleted, then only registered users of the

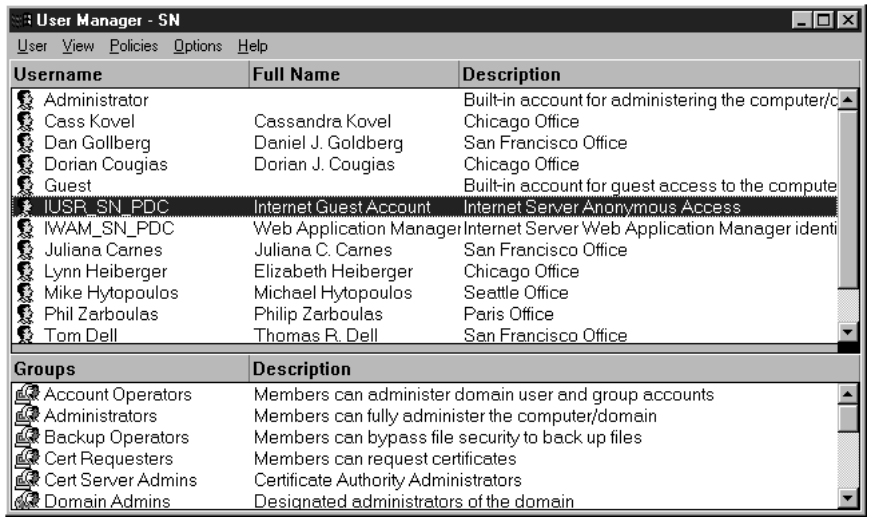

Figure 7.21 *Accounts Permitting Anonymous Access in User Manager for Domains.*

Windows NT Server will be permitted access to the IIS. This is handy for secure environments, but causes problems for public sites.

To enable or disable anonymous access, launch the Internet Service Manager (Microsoft Management Console) application from the Microsoft Information Server program group in the Windows NT 4.0 Option Pack program group. Here, open the FTP Properties and/or Web Properties dialog box, then select the Allow Anonymous Connections checkbox under the Security Accounts tab, as shown in Figure 7.22.

The IUSR account appears in the Username field by default. This can be changed using the Browse button should you wish to use the permissions of another account in the Windows NT users and groups database. If you do this, you must then also set the chosen account's corresponding password, or select the Enable Automatic Password Synchronization checkbox to copy it from the user and group database automatically.

If you select the Allow only anonymous connections checkbox, only guest access is permitted. This ensures that only those permissions assigned to the anonymous account can be used, regardless of the permissions a given user's account might have.

To provide low security for public sites, enable anonymous access and the IUSR account. To provide high security for private sites, disable anonymous access and disable or delete the IUSR account. Users will still be able to access the resource with valid user name/password combinations.

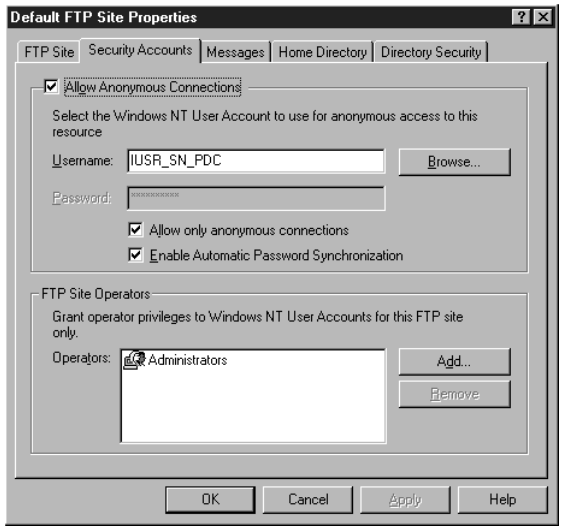

Figure 7.22 *Enabling Anonymous FTP Access.*

Troubleshooting Network Access

In addition to controlling access to resources user-by-user, the IIS also lets you control access host-by-host or network-by-network, much like a firewall.

In controlling network access, you need to apply one of two methodologies. In the first case, you deny specific hosts or networks access and permit access to everyone else. In the second case, you permit access to specific hosts and networks and deny access to everyone else. The method you choose will depend on the number of hosts you wish to include in your access controls. If you have a public Internet Web site, you might use the former method to deny access to certain problem hosts and networks. If you have a secure intranet, you will probably use the latter method to include only a few local hosts.

To grant or deny network access to a Web site, select the Edit button in the IP Address and Domain Name Restrictions field under the Directory Security tab of the Web Site Properties dialog box. This will open the IP Address and Domain Name Restrictions dialog box, as shown in Figure 7.23.

If you select the Granted Access radio button, all computers added to the exception pane will be denied access. If you choose the Denied Access radio button, all computers added to the exception pane will be granted access. You can add computers to the exception list by pressing the Add button to open the Grant/Deny Access On dialog box, as shown in Figure 7.24.

When connectivity problems are limited to specific hosts or networks, check these configurations to ensure that access is being allowed. This can be done on a directory level basis as well as for the entire site

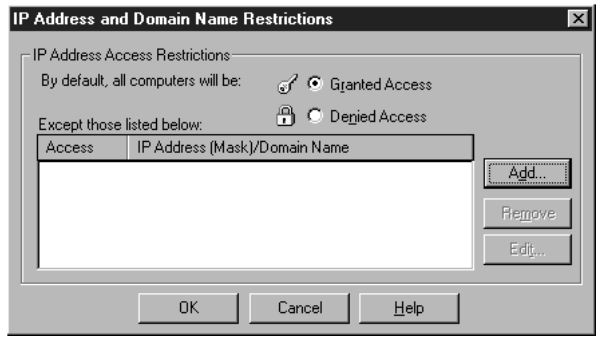

Figure 7.23 *Granting or Denying Web Site Access.*

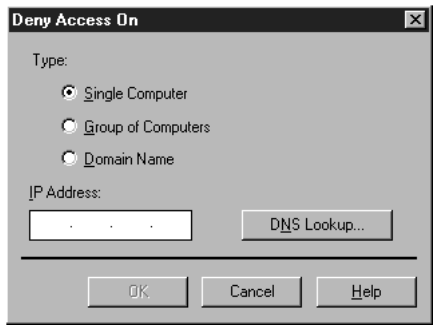

Figure 7.24 *Adding Computers to the Exception List.*

Troubleshooting Logons

Problems with logons generally have simple solutions. When registered users cannot log on to the IIS, try the following:

- Make sure they are using the right user name.
- Make sure they are using the right password.
- Make sure the Caps Lock is off. Passwords are case sensitive.
- Try logging on from the workstation using another account. If successful, recheck the user's settings in the User Manager for Domains application. It might be that the user's group memberships have changed or that a change in group rights is restricting the user. You might also check System Policy Editor to see if restrictions are being applied to the user. If unsuccessful, try logging in from another workstation. If that fails, you might need to repair the user accounts database on the Windows NT Server.

Troubleshooting Port Numbers

Web browsers and FTP clients are designed to look for these services at certain port numbers by default (80 and 21, respectively). For added security, you can effectively hide these services by simply changing the port number. This can be done in the TCP Port field of the Web and FTP properties dialog boxes, as shown in Figure 7.25.

If you do this, however, be prepared to face some support issues as users are unable to find the sites without explicitly adding the new port numbers. In the case of Web browsers, you might want to include this information for the default home page. For Internet Explorer, this can be done by

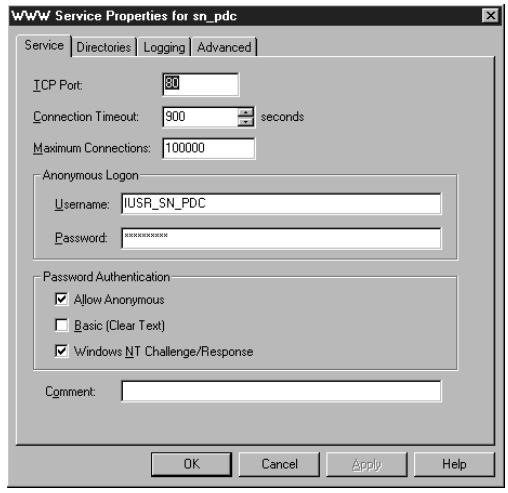

Figure 7.25 *Changing the WWW Service Port Number.*

choosing the Internet Options command under the View menu and modifying the Home page field under the General tab, as shown in Figure 7.26.

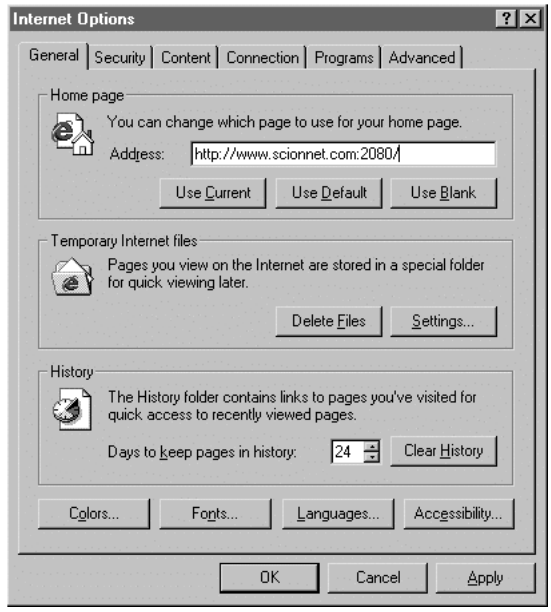

Figure 7.26 *Adding a Port Number to the Default Home Page URL in Internet Explorer.*

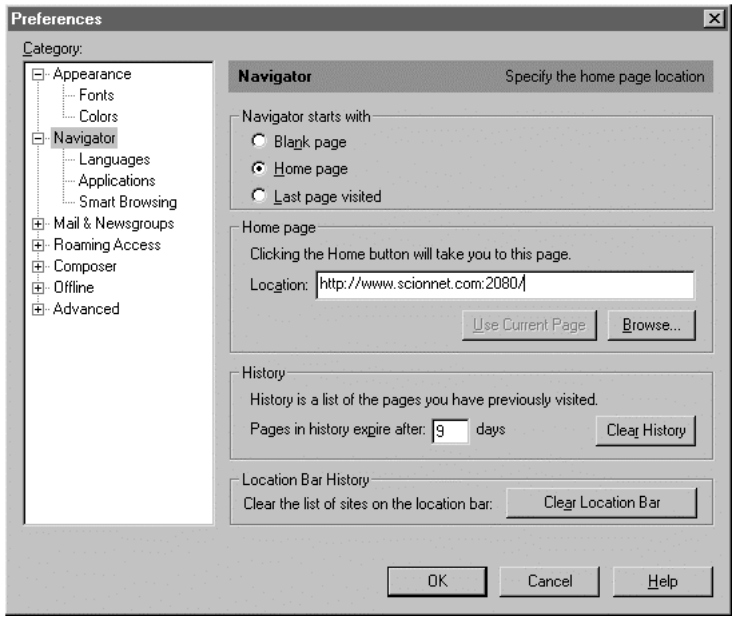

Figure 7.27 *Adding a Port Number to the Default Home Page URL in Netscape Communicator.*

For Netscape Navigator, this can be done by choosing the Preferences command under the Edit menu and modifying the Home page field under the Navigator tab, as shown in Figure 7.27.

You should use a number greater than 1024 as the new port number. Numbers under 1024 are reserved.

Setting NTFS Permissions

In addition to the security controls that restrict access to the Web and FTP sites as a whole, you should also be aware of NTFS permissions that can be set at the directory and file level. If these permissions are not configured correctly, access might be restricted to users who need it or granted to users who should not have it.

Permissions that can be assigned to directories are as follows:

- **No Access**. This choice permits users to see a shared directory, but not its file list.
- **List**. This choice permits users to see a directory's file list, but not access its contents.
- **Read**. This choice permits users to view subdirectory and file names, open subdirectories and files, and run applications. They cannot make changes, however.
- **Add**. This choice permits users to see a shared directory and copy data into it, but they cannot view the contents of the directory. This type of directory is often referred to as a "drop box."
- **Add & Read**. This choice permits users to view subdirectory and file names, read files, and save new files. They cannot make changes to existing files, however.
- **Change**. This choice permits users to view subdirectory and file names, open subdirectories and files, create subdirectories and files, delete subdirectories and files, modify file data, and run applications. They cannot alter permissions, however.
- **Full Control**. This choice permits users to view subdirectory and file names, open subdirectories and files, create subdirectories and files, delete subdirectories and files, modify file data, and run applications. They can also alter permissions and take ownership.

Permissions that can be assigned to files are:

- **No Access**. This choice permits users to see a file name and its attributes, but not open it.
- **Read**. This choice permits users to read from a data file or launch an application. They cannot make changes, however.
- **Change**. This choice permits users to read from a data file or launch an application, as well as modify or delete them.
- **Full Control**. This choice permits users to read from a data file or launch an application, as well as modify or delete them. They can also alter permissions and take ownership.

Windows NT also makes available two custom permissions levels: *Special Directory Access* and *Special File Access*. These allow you to create your own combinations from the six access permissions listed in Table 7.2.

Table 7.2 *NTFS Directory and File Permissions*[*]

Security	Directory	File
No Access	N/A	N/A
List	RX	N/A
Read	RX	RX
Add	WX	N/A
Add & Read	RXWD	RX
Change	RXWD	RXWD
Full Control	RXWDPO	RXWDPO

[*] N/A=not applicable, R = Read, W = Write, X = Execute, D = Delete, P = Change Permissions, O = Take Ownership.

To establish permissions for a file or subdirectory, first select it in My Computer or Explorer, then choose the Properties command from the File menu. Next, switch to the Security tab and press the Permissions button to open the Permissions dialog box. Here use the Add button to open the Add Users and Groups dialog box, as shown in Figure 7.28.

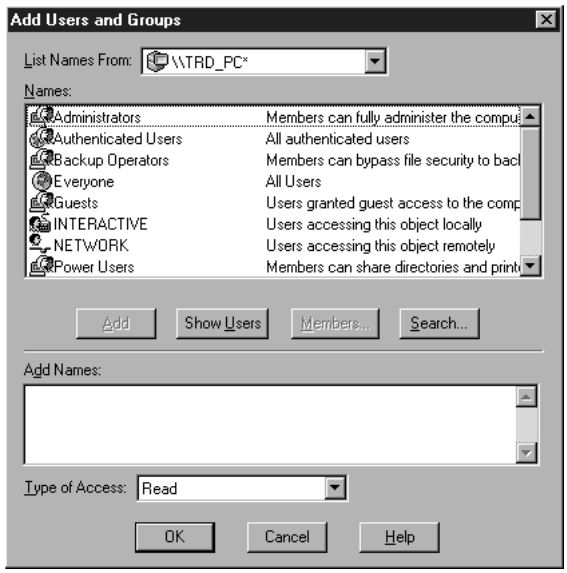

Figure 7.28 *Add Users and Groups Dialog Box.*

Here you are given the option of adding groups. To add an individual user, press the Show Users button to see users listed as well.

When designating permissions for files, two additional options are available. The Replace Permissions in Subdirectories checkbox modifies the permissions on subdirectories in a directory from the top level down, but not those of files. The Replace Permissions on Existing Files checkbox extends modified directory permissions to files, but not to subdirectories or the files they contain.

Note that you may create situations in which users are granted different sets of permissions by virtue of the fact that they are members of multiple groups. This does not create conflicts, as all permissions are cumulative. The exception is the No Access permission, which will override all the other permissions.

Using SSL and Server Certificates

With the Secure Socket Layer (SSL) protocol, secure, encrypted connections can be created between the server and client using the public key encryption system. This type of security should be used whenever private data, such as credit card information, is passed over the Internet.

SSL has two protocol layers. The first layer, the *SSL Handshake Protocol*, is used at the beginning of the client-server communications process to establish the encryption algorithm. The second layer, the *SSL Record Protocol*, is used to handle the encapsulation of data communicated over TCP and other higher-level protocols. This capability allows SSL to operate independent of applications, services, and data types. In a typical Web server to Web browser connection, SSL works as follows.

1. The Web browser requests a URL to a secured resource on the server, initiating the communications process.
2. The server sends a certificate to the Web browser. This contains the Web site's unique digital identification. It might also request a certificate from the Web browser.
3. The Web browser sends a certificate to the server, if requested.
4. The Web browser attempts to verify the server's certificate with a public key. If the certificate is verified, the Web browser requests an encryption specification, called the *session key*, from the server. This is encrypted using the Web browser's private key.
5. The Web server attempts to verify the Web browser's certificate with a public key, if requested.

6. The Web server receives the session key, which it decrypts using the Web browser's public key. It then modifies its encryption specification to match that requested by the Web browser.
7. The Web server and Web browser begin normal communication over the encrypted connection.

By design, if any of these steps is executed incorrectly, SSL communications will fail. It is mandatory for both the client and server to be able to supply the correct encryption, certificates, and other information. The digital signature process just described uses the default key pair installed in the browser to set up the SSL connection. The key exchange procedure is slightly different when client certificates are not required. When using client certificates the session key is sent by encrypting with the recipient's public key, so the information can only be deycrypted by the recipient, a subtle difference.

MCSE 7.3 Troubleshooting Resource Access

In this section, you will learn to troubleshoot resource access problems that can be caused by incorrect IP configurations, DHCP settings, and host name resolutions.

Troubleshooting With IPCONFIG

The manual configuration of TCP/IP leaves a lot of room for human error, and is commonly responsible for clients failing to connect to the server. One way around these issues is to have the Windows NT DHCP Server provide each client's TCP/IP information. If errors still occur at the client end, you can use the IPCONFIG utility to troubleshoot them.

If you want to know which network settings a DHCP server has leased to a Windows- or DOS-based client computer, you may type the following command at the command prompt:

```
IPCONFIG /all
```

Here you can verify the TCP/IP information, including host name, DNS servers, IP address, subnet mask, and the duration of the lease, as shown in Figure 7.29.

If there is a problem, you may see that the client computer has an invalid address of 0.0.0.0 while the DHCP server has a broadcast address of 255.255.255.255. This often means the client computer has no connectivity

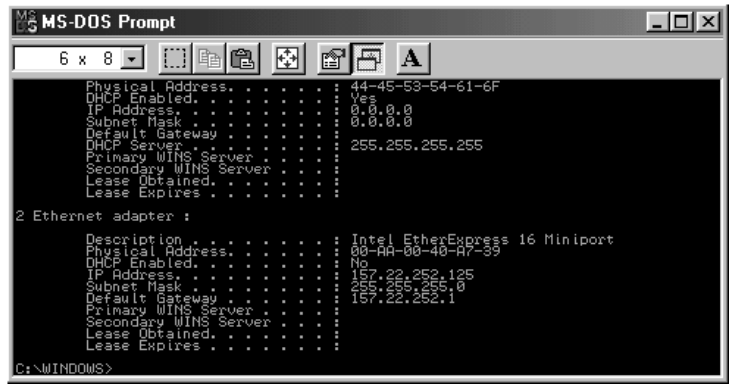

Figure 7.29 *Viewing Client Configuration with IPCONFIG.*

to a DHCP server, in which case you should release the client's IP address and then try to lease a new IP address. To do this, type the next sequence of commands from the DHCP client computer at a command prompt.

```
IPCONFIG /release

IPCONFIG /renew
```

If there is a DHCP server present on the network, the client should be granted a new lease.

You can also use the WINIPCFG utility to view the IP configuration and renew the lease on a Windows-based computer, as shown in Figure 7.30.

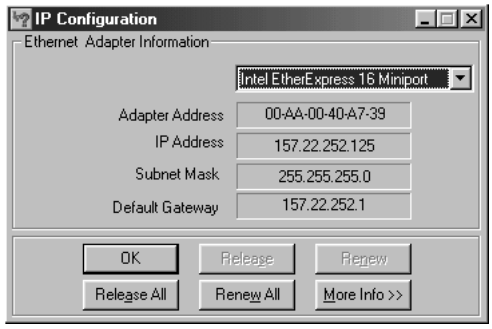

Figure 7.30 *Viewing Client Configuration with WINIPCFG.*

Troubleshooting With PING

The PING utility verifies a connection by sending Internet Control Message Protocol (ICMP) packets to a remote host and listening for echo reply packets. PING waits for up to one second for each packet sent and displays the number of packets transmitted and received. It sends four packets by default, but you can change the default (see Figure 7.31).

To test a connection, you can use the PING command with an IP address, a host name, or a computer name. It is best to use the IP address initially to isolate the problem as related to connectivity versus host name resolution. Useful PING troubleshooting procedures include the following.

PINGING THE LOOPBACK ADDRESS

To find out if the DOS or Windows client's TCP/IP protocol stack is working properly, test the configuration of the computer by typing:

```
PING localhost
```

Localhost is a reserved host name that maps to a reserved IP address (127.0.0.1), which represents your computer. If pinging your local host is successful, you will receive four replies from IP address 127.0.0.1, as shown in Figure 7.32.

If the PING command is unsuccessful, you will receive a message telling you "localhost is unknown." If unsuccessful, make sure that the TCP/IP protocol is installed on the computer, that the network adapter is properly installed, and that the TCP/IP protocol has been bound to the network

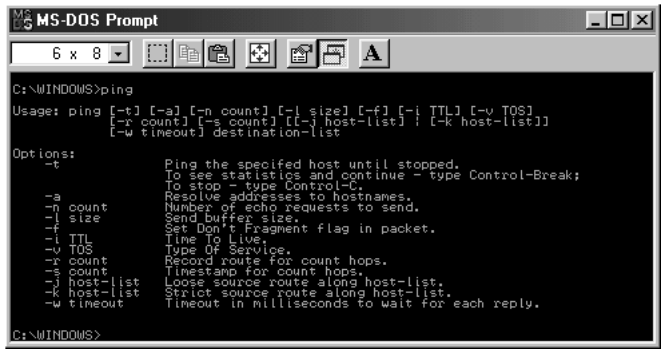

Figure 7.31 *Viewing Options for the PING Utility.*

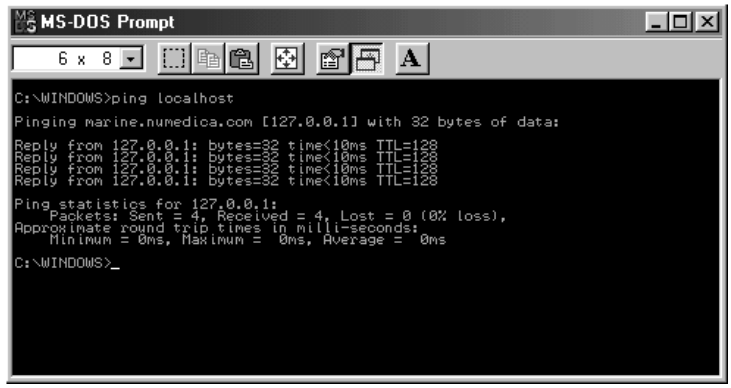

Figure 7.32 *Successfully Pinging the Local Host.*

adapter. Also check the system log in Event Viewer to make sure all services have started correctly.

Sometimes it is necessary to reboot the client computer to solve this problem. Another trick is to re-install the TCP/IP protocol altogether.

PINGING THE LOCAL HOST

You can further verify the configuration of the local host by using the PING command with the actual IP address of the local computer. If all is well, you should get immediate replies, as shown in Figure 7.33.

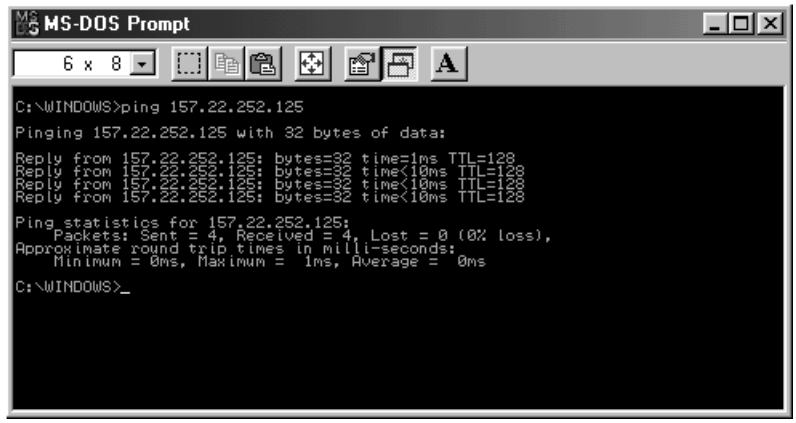

Figure 7.33 *Successfully Pinging the Local Host.*

If this test is unsuccessful, check to make sure that the correct IP address was either configured manually or received from the DHCP server.

Because this test does not send packets out on the network, it will not tell you if the local host has proper network connectivity.

PINGING A REMOTE HOST ON THE SAME SUBNET

You can verify that network communications are possible between your computer and another host on your local subnet by using the PING command with the IP address of that other computer. If all is well, you should see packets going out on and coming back over the network (see Figure 7.34).

If the test is unsuccessful, check to make sure you have the proper IP addresses, subnet masks, and gateway addresses configured on both hosts.

This test will only tell you if connectivity is possible on the local subnet. It will not tell you if communications are possible with hosts on another subnet or the Internet.

PINGING THE DEFAULT GATEWAY

You can verify that network communications are possible between your computer and the gateway by using the PING command with the IP address of the router. If all is well, you should see packets going out on and coming back over the network, just as when you pinged the remote host. If there is a problem, the packets will not be returned in the required time and you will see the messages shown in Figure 7.35.

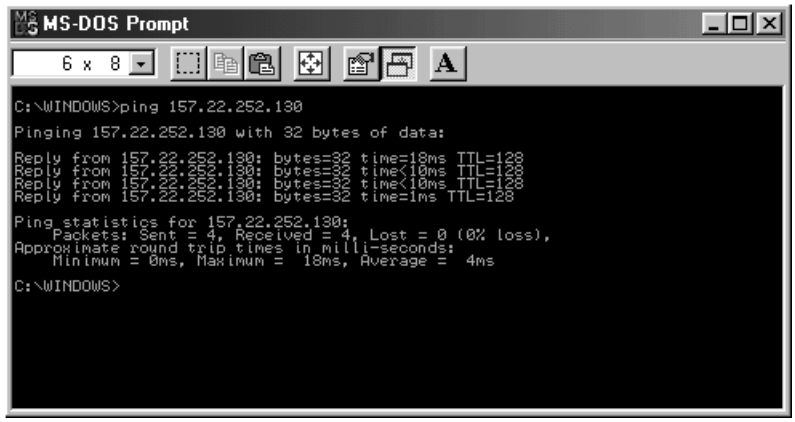

Figure 7.34 *Successfully Pinging Another Local Host.*

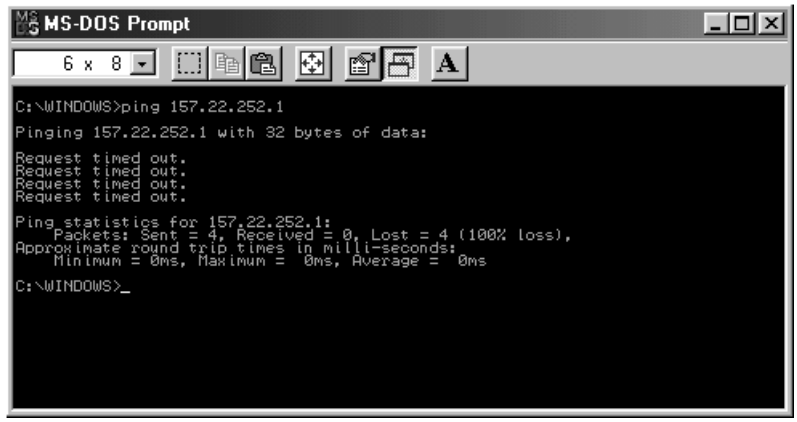

Figure 7.35 *Unsuccessfully Pinging the Gateway.*

If the test is unsuccessful, you should first make sure the router is available (e.g., that it is powered up and connected to the network). Check again to make sure the local host is configured with the correct subnet mask and gateway address. You might also need to verify that the router is configured properly. Routers have multiple IP addresses for the multiple subnets they reside on. The port that is connected to the subnet on which your local host resides must have an IP address and subnet mask that is valid for your subnet. Other ports must have IP addresses and subnet masks that are valid for those subnets and/or the Internet. You can verify all of these ports by pinging each of their addresses.

PINGING A REMOTE HOST ON ANOTHER SUBNET

You can verify that network communications are possible between your computer and a remote host on another subnet or the Internet by using the PING command with the IP address of that remote host. Again, if all is well, you should see packets going out on and coming back over the network. If there is a problem, the packets will not be returned in the required time and you will see time-out messages (see Figure 7.35).

If the test is unsuccessful, and you have already performed the previous tests to determine that local connectivity is possible, then the problem might lie with routers or hosts beyond your network. This type of problem can often be tracked down using another utility: TRACERT.

Troubleshooting With TRACERT

If you can ping your default gateway but not a remote host, employ the TRACERT (Trace Route) utility next. It displays the Fully Qualified Domain Name (FQDN) and IP address of each gateway along the route to a remote host. You can use TRACERT with either the host name or IP address of the remote computer, as shown in Figure 7.36.

Document the information that the TRACERT command returns when the remote host is available. Later, if the remote host is not available, you can compare the information returned by TRACERT with the earlier results to determine which gateway is down.

If your organization uses a proxy server for access to the Internet, you may not be able to use PING or TRACERT for hosts beyond your intranet.

Troubleshooting With NETSTAT

The NETSTAT utility is used to list which TCP/IP ports are used during communications sessions, as shown in Figure 7.37. With it you can quickly determine if certain ports are not being accepted across the link, perhaps because they are being blocked at a firewall.

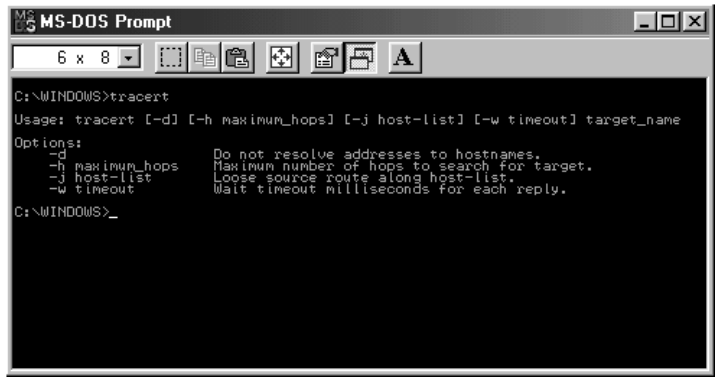

Figure 7.36 *Viewing Options for the TRACERT Utility.*

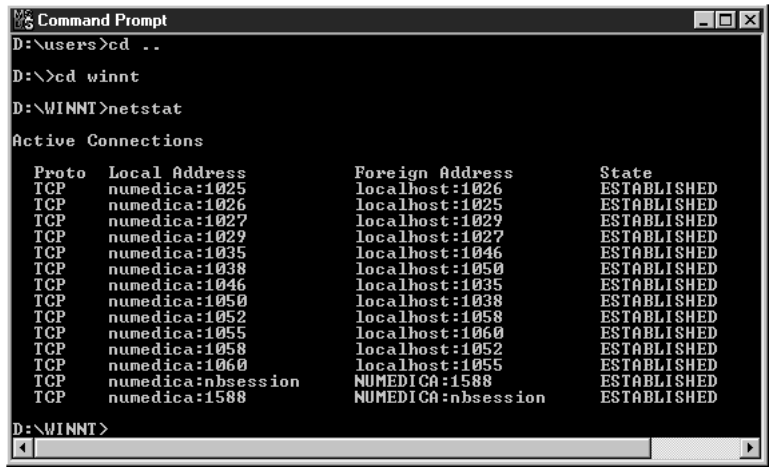

Figure 7.37 *Viewing Results from the NETSTAT Utility.*

If you find this is a problem, contact the administrator of the firewall to determine a solution.

Troubleshooting Name Resolution

If you have used PING and other utilities to determine that TCP/IP connectivity is functioning, but you are still unable to access a resource via a host name or computer name, it is time to troubleshoot name resolution. For example, you might successfully ping a host using the IP address, but fail when you attempt to use a host name, as shown in Figure 7.38.

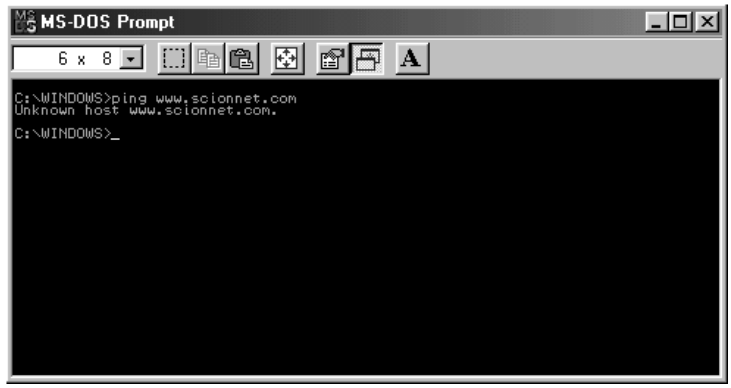

Figure 7.38 *Unsuccessful Attempt to Ping Hostname.*

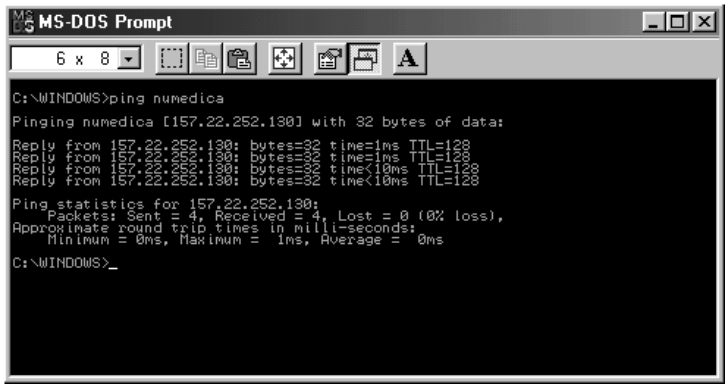

Figure 7.39 *Successful Attempt to Ping by Hostname.*

A proper resolution would match the host name with the IP address and successfully execute the PING command, as shown in Figure 7.39.

Resolution refers to the process by which Windows maps host names, which make sense to humans, with IP addresses, which make sense to computers. Host name resolution for Windows-based computers occurs in a couple of ways. The TCP/IP host name (e.g., "marine_PC.scionnet.com") can be mapped to an IP address by a DNS server or a HOSTS file. The NetBIOS computer name (e.g., "Marine's PC") can be mapped to an IP address by a WINS server or LMHOSTS file.

RESOLVING NETBIOS COMPUTER NAMES

NetBIOS names are assigned to Windows NT and Windows 98 client computers. When such a computer searches for a resource, it resolves the computer name with an IP address by performing the following steps.

1. The client computer looks in its local name cache to see if the address mapping information is there.
2. If the address mapping information is not in the local name cache, and the client computer is configured to use WINS, it will query the WINS server.
3. If the WINS server is not able to provide the address mapping information, the client computer sends a broadcast query onto the local subnet (broadcast packets typically do not travel across routers).
4. If the client computer receives no response to its query, it will look for the address mapping information in the LMHOSTS file.

5. If the client computer cannot find address mapping information in the LMHOSTS file, it will look for it in the HOSTS file.
6. If the client computer cannot find address mapping information in the HOSTS file, and the client has been configured to use DNS, it will query the DNS server.

The maximum length of a NetBIOS name is 15 characters. If a name longer than 15 characters is specified, the client computer will look to a DNS server before a WINS server or HOSTS file for address mapping information.

You can use the HOSTNAME utility to view the computer name of the local host. This is the name as configured under the Identification tab of the Network Control Panel application.

You can use the NBSTAT utility to view statistics relating to NetBIOS over TCP/IP parameters, as shown in Figure 7.40.

You can verify NetBIOS name resolution by establishing a session with another host. For example, you can map a drive or execute a Net Use command (see Figure 7.41).

If you are unable to establish a session, check to see that the same NetBIOS scope IDs are being used by both hosts. The use of NetBIOS *scopes* permits the creation of logical TCP/IP networks that are invisible to one another. If your network is configured in this manner, you will need to configure the Scope ID field under the WINS Configuration tab in the TCP/IP

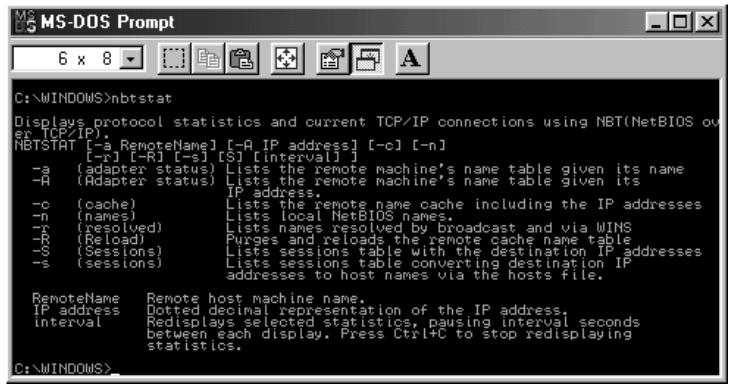

Figure 7.40 *Viewing Options for the NBTSTAT Utility.*

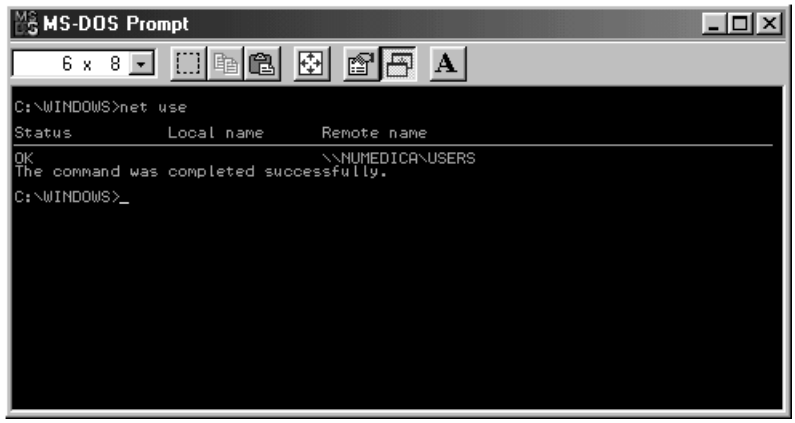

Figure 7.41 *Successfully Executing a NET USE Command.*

Properties dialog box of the Network Control Panel application to be able to communicate with other hosts in your scope, as shown in Figure 7.42. Hosts can only communicate if they belong to the same NetBIOS scope.

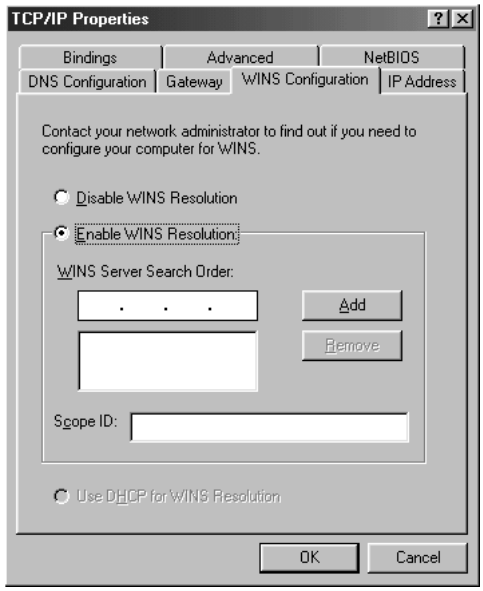

Figure 7.42 *Configuring the Scope ID Field for NetBIOS.*

Another area to check is the local name cache. Make sure that its entries are correct using the NBTSTAT utility with the –C switch. If there is old incorrect data, reload the cache (–R switch) and try the session again.

If there is no problem with the name cache, verify that the correct WINS server information has been configured on the client computer. This information can be viewed in the TCP/IP Properties dialog box of the Network Control Panel application or by using IPCONFIG with the /all switch. You can also verify the WINS database on the server using the WINS Manager application.

If there appears to be no problem with either the local name cache or WINS, take a look at the LMHOSTS file, as shown in Figure 7.43.

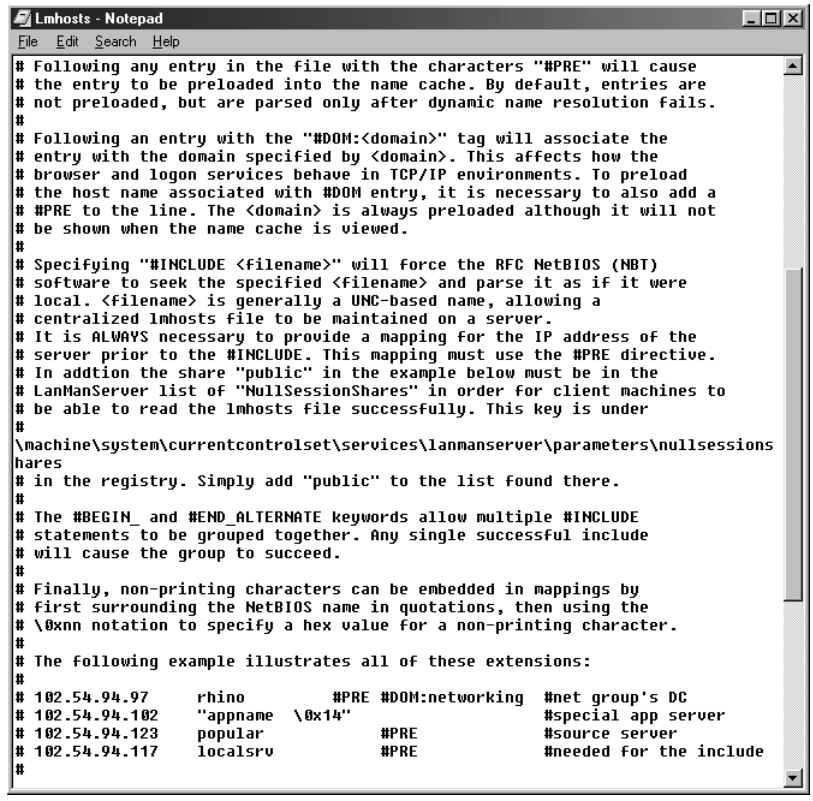

Figure 7.43 *Viewing the LMHOSTS File.*

Problems can occur with the LMHOSTS file if it is moved. This file must be located in the following directory path on Windows NT computers:

```
\WINNT\System32\drivers
```

The LMHOSTS file is located in the \WINDOWS directory on Windows 98 computers.

Make sure that the correct names and IP addresses are listed in the LMHOSTS file. If there are multiple entries for the same computer, only the first entry will be used. Also ensure that the correct format is used for LMHOSTS entries and extensions, as shown in Table 7.3.

Table 7.3 *LMHOSTS Extensions*[*]

Syntax	Description
#	Generally used to denote the start of a comment.
#PRE	Causes the entry to be preloaded into the name cache. By default, entries are parsed only after dynamic name resolution fails.
#DOM:<domain>	Associates the entry with the domain specified by <domain>. This affects how the browser and logon services behave in TCP/IP environments. To preload the host name associated with #DOM entry, it is necessary to also add a #PRE to the line. The <domain> is always preloaded although it will not be shown when the name cache is viewed.
#INCLUDE <filename>	Forces the RFC NetBIOS (NBT) software to seek the specified file and parse it as if it were local. <filename> is generally a UNC-based name, allowing a centralized LMHOSTS file to be maintained on a server. It is *always* necessary to provide a mapping for the IP address of the server prior to the #INCLUDE. This mapping must use the #PRE directive.
#BEGIN_ALTERNATE #END_ALTERNATE	These keywords allow multiple #INCLUDE statements to be grouped together. Any single successful #INCLUDE will cause the group to succeed.
\0xnn	Denotes non-printing character support. These can be embedded in mappings by first surrounding the NetBIOS name in quotations, then using the \0xnn notation to specify a hex value for a non-printing character.

[*] Compiled from Microsoft's sample LMHOSTS file.

RESOLVING TCP/IP HOST NAMES

Host names are assigned to Windows NT Server computers that run TCP/IP services, such as the IIS, and to other non-Windows computers such as

The use of the LMHOSTS file is optional. It is meant to provide a static way of saving name resolution information to supplement the more dynamic WINS and network broadcast methods.

UNIX machines. When a Windows computer searches for a resource, it resolves the host name with an IP address by performing the following steps.

1. The client computer looks in its local name cache to see if the address mapping information is there.
2. If the address mapping information is not in the local name cache, it will look for it in the HOSTS file.
3. If the client computer cannot find address mapping information in the HOSTS file, and the client has been configured to use DNS, it will query the DNS server
4. If the DNS server is not able to provide the address mapping information, and the client computer is configured to use WINS, it will query the WINS server.
5. If the WINS server is not able to provide the address mapping information, the client computer sends a broadcast query onto the local subnet (broadcast packets typically do not travel across routers).
6. If the client computer receives no response to its query, it will look for the address mapping information in the LMHOSTS file.

The last three steps refer to sources that contain NetBIOS name resolution data. They are also checked, however, because it is possible that they might contain host name resolution data.

You can verify host name resolution by establishing a socket connection with another host. For example, you could try to establish a Telnet, FTP, or Web connection (see Figure 7.44).

Verify that the correct DNS server information has been configured on the client computer. This information can be viewed in the TCP/IP Properties dialog box of the Network Control Panel application. You can also verify the WINS database on the server using the DNS Manager application.

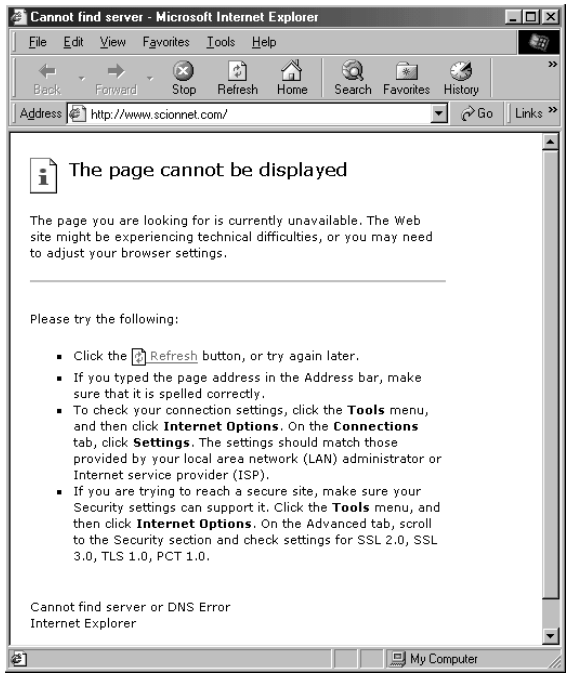

Figure 7.44 *Unsuccessful Attempt to Open a Web Server Connection.*

If there appears to be no problem with the DNS server, take a look at the HOSTS file, as shown in Figure 7.45.

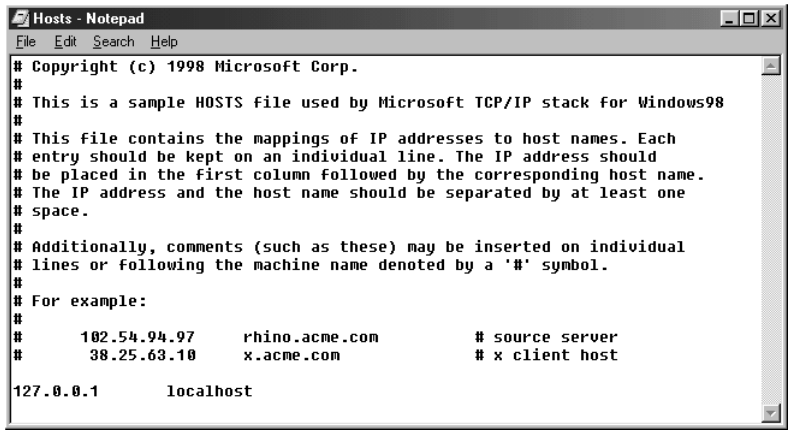

Figure 7.45 *Viewing the HOSTS File.*

Problems can occur with the HOSTS file if it is moved. This file must be located in the following directory path on Windows NT computers:

```
\WINNT\System32\drivers
```

The HOSTS file is located in the \WINDOWS directory on Windows 98 computers.

Make sure that the correct names and IP addresses are listed in the HOSTS file. Also ensure that the correct format is used for HOST entries. As noted in Microsoft's sample file, each entry should be kept on an individual line. The IP address should be placed in the first column followed by the corresponding host name. The IP address and the host name should be separated by at least one space. Additionally, comments may be inserted on individual lines or following the machine name and are denoted by a number (#) symbol.

The use of the HOSTS file is optional. It is meant to provide a static way of saving host name resolution information to supplement the more dynamic DNS.

Study Break

Study Break: Using PING

Practice what you have learned by using the PING utility to test TCP/IP connectivity.

First, use PING with the "localhost" command to verify the configuration of the local host. Next, use PING with the IP address of a remote host on the same subnet to test local network connectivity. Next, use PING with the IP addresses of the ports on the router to test gateway connectivity. Finally, Use PING with the IP address of a host on the Internet to test remote network connectivity.

MCSE 7.4 Troubleshooting Index Server Queries

In this section, you will learn to troubleshoot the Index Server in general and problems that might occur during the query process in particular.

Troubleshooting Index Server Problems

In most cases, the Index Server performs troubleshooting functions automatically without requiring administrator intervention. There is a recovery function that executes should the cache become corrupted, for example. Such events are written to the application log, as will be described further on.

Starting the Index Server does not require administrator intervention either. The service starts automatically when the IIS is launched, unless its startup parameters have been explicitly set to manual. Even when startup is set to manual, the Index Server starts automatically when a query is made.

You can start and stop the Index Server manually using the Services application from the Control Panel program group, as shown in Figure 7.46.

Perhaps the most common problem that can affect Index Server operations is disk space. When the disk drive is filled, the Index Server pauses all indexing operations and writes a message to the Event log. You should therefore monitor the log and drive space allocations regularly.

Another issue that can arise involves *word weighting*, which refers to the way in which words are indexed for importance. This can be done in several ways. For example, a word that appears in a title has a higher weight than one that is located in body text. How many times a word appears—called the *term*—has a weight. The proximity of multiple words to each other has a weight. Finally, the density of the word has a weight. (*Density* refers to the result of dividing the number of times a word appears by the total number of words in the data in which it appears.)

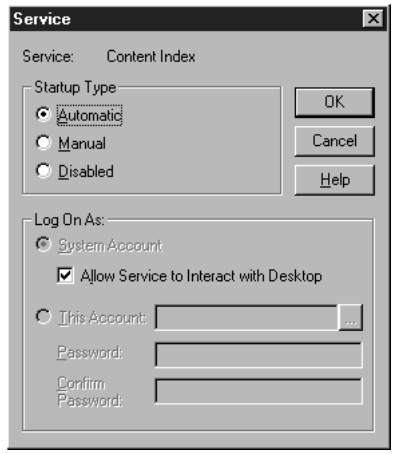

Figure 7.46 *Starting and Stopping the Index Server.*

Word weighting is handled by the WAISINDX.EXE utility. It also determines which words will be indexed and where the actual data is found. In general, WAISINDX creates seven indices for each data file which, combined, equal about 110 percent of the data file's size. If you add new records to the data, WAISINDX must be run to create new indices that include this data.

Troubleshooting Query Errors

Table 7.4 lists the messages that can be returned when an error occurs during the query process.

Table 7.4 *Index Server Query Syntax Error Messages**

Error Message	Description
Expecting closing parenthesis ')'	Parenthesis were mismatched.
Expecting closing square bracket ']'	Opening square bracket was not followed by a closing bracket.
Expecting comma	Reserved token or end-of-string was before the closing brace of a vector property.
Expecting currency	Property type DBTYPE_CY received incorrect input. The correct format is #.#.
Expecting date	Property type DBTYPE_DATE received incorrect input. The correct format for absolute dates is yyy/mm/dd, yyy/mm/dd hh:mm:ss The correct format for relative dates is (-#y,-#m, -#w,-#d, -#h, -#n, -#s).
Expecting end of string	More input was present beyond the restriction that was parsed.
Expecting GUID	Property type DBTYPE_GUID, Globally Unique Identifier (GUID), received incorrect input. The correct format is xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx.
Expecting integer	Property of an integer type, such as DBTYPE_I4, received a nonnumeric value or vector weight.
Expecting phrase	Special token was received instead of plain text.
Expecting property name	No legal property name was found after an @ sign.
Expecting real number	Property of a real type, such as DBTYPE_R4, received a nonnumeric value.
Expecting regular expression	Special token was received instead of text while in regular expression parsing mode.
The file <file_name> is on a remote UNC share. .IDQ, .IDA, and .HTX files cannot be placed on a remote UNC share.	Files ended in .IDQ, .IDA, and .HTX are on an Universal Naming Convention (UNC) share, which is not permitted.

Table 7.4, continued.

Error Message	Description
Invalid literal	Query has incorrect format.
No such property	Property specified after a #, $, or @ sign does not exist. The property is not a default. The property is not specified in the [Names]section of the .IDQ file.
Not yet implemented	Index Server feature is not yet functional.
Out of memory	Processing a CiRestriction exceeded available memory.
Regular expressions require a	Property of a nontextual type, such as DBTYPE_I4 or received property of type string DBTYPE_GUID, was selected for regular-expression mode.
Unexpected end of string	Query is missing a question mark.
Unsupported property type	Property type is not yet implemented.
Weight must be between 0 and 1000	Query term weight is outside of the legal range.

* Compiled from the IIS 4.0 help file ixerrysn.htm.

Troubleshooting IDQ Errors

As previously described, the .idq file is used to define query parameters, such as the scope of the search and restrictions on its format. The .idq file contains a [QUERY] section and, optionally, a [NAMES] section. The latter, which is rarely used, can contain non-standard column names as referred to in the query. The former contains query parameters, variables, and conditional expressions. Syntax errors within the .idq file, such as those listed in the following Table 7.5, are returned by the CiErrorMessage variable and can be read in .htx pages.

Table 7.5 *IDQ File CiErrorMessage Errors*[*]

Error Message	Description
The catalog directory cannot be found in the location specified by CiCatalog= in the file <file_name>	CiCatalog parameter did not contain a valid index catalog name.
DBTYPE_BYREF must be used with DBTYPE_STR, DBTYPE_WSTR, DBTYPE_GUID, or DBTYPE_UI1 types	DBTYPE_BYREF type was not used with an indirect type in the [Names] section.

Table 7.5, continued.

Error Message	Description
DBTYPE_VECTOR or DBTYPE_BYREF used alone	VECTOR and BYREF property modifiers were not used with a type, as is required.
Duplicate column, possibly by a column alias, found in the CiColumns= specification in the file <file_name>	Property was named multiple times in the CiColumns line.
Duplicate property name	Property was named multiple times in the [Names] section.
Expecting closing parenthesis	Opening parenthesis were not followed by closing parenthesis in the [Names] section.
Expecting GUID	Entry in [Names] section had incorrect format.
Expecting integer	Entry in [Names] section had incorrect format.
Expecting property name	Entry in [Names] section had incorrect format.
Expecting property specifier	Property specifier in [Names] section was invalid or missing.
Expecting SHALLOW or DEEP in .IDQ file <file_name> on Line CiFlags=	CiFlags parameter had incorrect value.
Expecting TRUE or FALSE in .IDQ file <file_name> on line CiForceUseCi=	CiForceUseCi parameter had incorrect value.
Expecting type specifier	Entry in [Names] section had incorrect format.
Failed to set property name	Resource failure occurred, such as running out of memory.
The file <file> is on a network share. .IDQ, .IDA, and .HTX files cannot be placed on a network share	Files ended in .IDQ, .IDA, and .HTX are on a network share, which is not permitted. They must be moved to the virtual root on the local computer.
The .HTX file specified could not be found in any virtual or physical path	CiTemplate parameter specified a file that could not be found.
The .IDQ file <file_name> contains a duplicate entry on the line <line>	Parameter in the [Query] section was given multiple times.
The .IDQ file <file_name> could not be found	.IDQ file was not found in the location specified.
An invalid CiScope= or CiCatalog= was specified in the file <file_name>	CiScope or CiCatalog conditions were incorrect.
Invalid GUID	Entry in [Names] section had incorrect format.
An invalid locale was specified on the CiLocale= line in .IDQ file <file_name>	CiLocale parameter was not recognized.
Invalid property found in the CiColumns= specification in file <file_name>	Property specified by the CiColumns parameter was not standard and was not listed in the [Names] section.

Table 7.5, continued.

Error Message	Description
Invalid property found in the CiSort= specification in file <file_name>	Property specified by the CiColumns parameter was not standard and was not listed in the [Names] section.
An invalid sort order was specified on the CiSort= line in the file <file_name>. Only [a] and [d] are supported	Sort-order value following the CiSort parameter was invalid. Permitted values are a for ascending and d for descending.
One or more output columns must be specified in the .IDQ file <file_name>	CiColumns parameter was missing. At least one output column must be specified.
Operation on line number of .IDA file <file_name> is invalid	.IDA file contained and unrecognized keyword.
The query failed because the Web server is busy processing other requests	The number of queries allowed was exceeded.
Read error in file <file_name>	I/O error occurred while file was being read.
A restriction must be specified in the .IDQ file <file_name>	CiRestriction parameter was missing.
A scope must be specified in the .IDQ file <file_name>	CiScope parameter was missing.
The template file cannot be found in the location specified by CiTemplate= in file <file_name>	CiTemplate parameter could not be used to locate a .HTX file.
A template must be specified in the .IDQ file <file_name>	CiTemplate parameter was missing.
Template for .IDA file <file_name> cannot have detail section	An illegal section was found in the .IDA file. Remove everything beginning with <%BeginDetail%> and ending with <%EndDetail%>.
Unrecognized type	Invalid type was specified.
You must specify MaxRecordsPerPage in the .IDQ File <file_name>	The CiMaxRecordsPerPage parameter is missing.

* compiled from the IIS 4.0 help file ixerridq.htm.

Using the Application Log

In many cases, the only way to determine what problems are occurring within the Index Server is to monitor the Windows NT application event log, shown in Figure 7.47.

Index Server errors, as listed in Table 7.6, appear in the Ci Filter Service category. These include problems with index corruption, insufficient resources, and indexing.

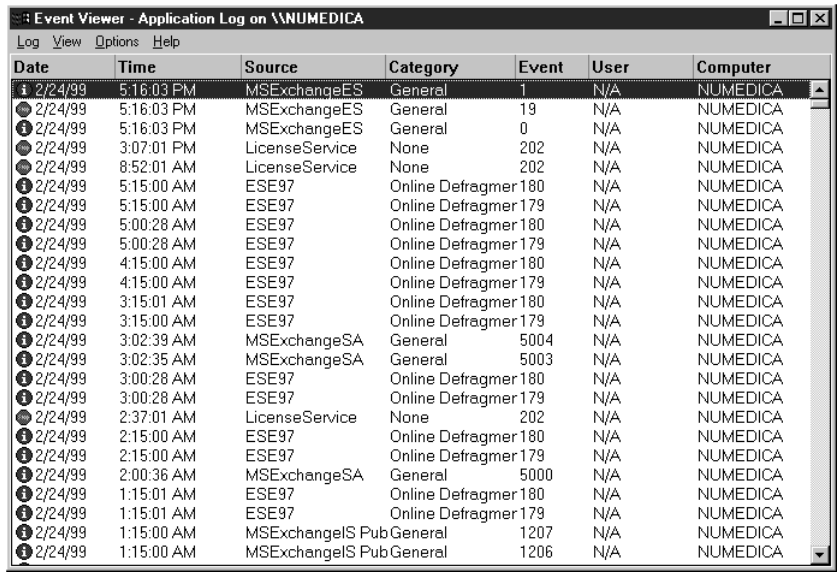

Figure 7.47 *Viewing the Windows NT Server Application Log.*

Table 7.6 *Ci Filter Service Error Messages*[*]

Error Messages	Description
Account <*user-id*> does not have interactive logon privilege on this computer. You can give <*user-id*> interactive logon privilege on this computer using the user manager administrative tool	The user did not have interactive logon privileges for the Index Server computer. Update the user's privileges with User Manager for Domains.
The CI filter daemon has prematurely stopped and will be subsequently restarted	The filter daemon Cidaemon.exe stopped unexpectedly. This can be caused by poorly written filters.
CI has started on <*catalog*>	This is an informational message that is logged when the Index Server is started successfully.
Class for extension <*extension*> unknown. Sample file: <*file_name*>	Files with the extension specified were filtered with the default text filter, adding unnecessary data to the index. Consider turning off filtering for this extension.
Cleaning up corrupted content index metadata on <*catalog*>. Index will be automatically restored by refiltering all documents.	A catastrophic data corruption error was detected on the specified catalog, which will be rebuilt. This can be caused by a hardware failure or (rarely) because of an abrupt shutdown or power failure.

Table 7.6, continued.

Error Messages	Description
Content index on <*catalog*> could not be initialized. Error <*number*>.	An unknown, possibly catastrophic, error occurred. Report the error number to Microsoft Technical Support, delete all files under <*catalog*>, and re-index.
Content index on <*catalog*> is corrupted. Please shut down and restart Web server.	A catastrophic data corruption error was detected on the specified catalog, which will be rebuilt. This is can be caused by a hardware failure or (rarely) because of abrupt shutdown or power failure. To recover, shut down and restart the Web server.
Content index corruption detected in component <*component*>. Stack trace is <*stack*>.	The content index was corrupted. Delete the catalog and start over. If the error recurs, remove and reinstall Index Server.
The content index could not filter file <*file*>. The filter operation was retried <*number*> times without success.	The specified document failed to filter. This indicates a corrupted document, corrupted properties, or in rare cases, a case in which the document was in use for a long time.
Content index on drive is corrupted. Please shutdown and restart the Content Index service (cisvc).	Stop and restart the service in the Services Control Panel application.
The content index filter for file "<*file*>" generated content data more than <*size*> times the file's size.	Filtering the document generated more output than is allowed. This can be caused by a poorly written filter, a corrupted document, or both.
The content index filter stopped while filtering "<*file*>". The CI daemon was restarted. Please check the validity of the filter for objects of this class.	Document filtering started, but did not finish before the timeout period expired. This is usually caused by a poorly written filter, a corrupted document, or both.
A content scan has completed on <*catalog*>.	The catalog was scanned successfully.
An error has been detected on <*catalog*> that requires a full content scan.	The catalog lost a change notification. This can be caused by a lack of disk space or hardware failure. The complete scope of the catalog will be scanned and all documents will be refiltered at a suitable time.
An error has been detected in content index on <*catalog*>.	The content index was corrupted. Delete the catalog and start over. Remove and reinstall Index Server if the error recurs.
An error has been detected on <*catalog*> that requires a partial content scan.	The catalog lost a change notification. This can be caused by a lack of disk space or hardware failure. The complete scope of the catalog will be scanned and all documents will be refiltered at a suitable time.
Error <*number*> detected in content index on <*catalog*>.	An unknown, possibly catastrophic error occurred. Report the error number to Microsoft Technical Support. To recover, delete all files under <*catalog*> and start over.

Table 7.6, continued.

Error Messages	Description
File change notifications are turned off for scope "<*scope*>" because of error <*number*>. This scope will be periodically rescanned.	Automatic change notifications for the specified directory scope could not be re-established. The Index Server will perform incremental scans to identify the document that changed the scope.
File change notifications for scope "<*scope*>" are not enabled because of error <*number*>. This scope will be periodically rescanned.	Automatic change notifications for the specified directory scope could not be re-established. This can happen with virtual roots that point to remote shares on file servers that do not support automatic change notifications. The Index Server will perform incremental scans to identify the documents that changed in the scope.
The filter service could not run since file <*file*> could not be found on your system.	An executable or DLL required for filtering, such as CiDaemon.exe, was not at the specified path.
A full content scan has started on <*catalog*>.	A complete rescan of the catalog was initiated.
<*number*> inconsistencies were detected in PropertyStore during recovery of catalog <*catalog*>.	Corruption was detected in the property cache, perhaps due to hardware failure or an unexpected shutdown. Recovery is automatic.
Master merge cannot be restarted on <*catalog*> due to error <*number*>.	A master merge could not be restarted because of the error noted.
Master merge cannot be started on <*catalog*> due to error <*number*>.	A master merge could not be started because of the error noted.
Master merge has been paused on <*catalog*>. It will be rescheduled later.	A master merge was temporarily halted, probably due to insufficient system resources.
Master merge has completed on <*catalog*>.	A master merge was completed.
Master merge has restarted on <*catalog*>.	A paused master merge was restarted.
Master merge has started on <*catalog*>.	A master merge was started.
Master merge was started on <*catalog*> because the amount of remaining disk space was less than <*number*>%.	A master merge was started because the amount of free space on the catalog volume dropped below the minimum threshold. You should increase the amount of disk space after the master merge completes.
Master merge was started on <*catalog*> because more than <*number*> documents have changed since the last master merge.	A master merge was started because the number of documents that changed since the last master merge exceeded the maximum threshold.
Master merge was started on <*catalog*> because the size of the shadow indexes is more than <*number*>% the disk.	A master merge was started because the amount of data in shadow indexes exceeded the maximum threshold.

Table 7.6, continued.

Error Messages	Description
Notifications are not enabled on <*pathname*> because this is a DFS aware share. This scope will be periodically scanned.	A virtual root points to a Distributed File System (DFS) share, which do not support notifications.
One or more embeddings in file <*file*> could not be filtered.	The file was filtered correctly, but several embedded objects could not be filtered. This is usually caused by embedded objects without a registered filter.
The path <*pathname*> is too long for Content Index.	A path is longer than the maximum number of 260 characters.
Please check your system time. It might be set to an invalid value.	The system time is invalid. For example, it is set to a date before January 1, 1980. When the system time is invalid the date may appear as 2096.
<*Process-Name*> failed to logon <*UserId*> because of error <*number*>.	The Index Server SearchEngine or CiDaemon failed to log on the specified user. The remote shares for which the UserId is used will not be filtered correctly. This can happen if either the password is wrong or the validity of the password could not be verified due to network errors.
PropertyStore inconsistency detected in catalog <*catalog*>.	Corruption was detected in the property cache, perhaps because of hardware failure or abrupt shutdown. Recovery is automatic.
Recovery is starting on PropertyStore in catalog <*catalog*>.	Corruption was detected in the property cache. Recovery is starting.
Recovery was performed successfully on PropertyStore in catalog <*catalog*>.	Corruption was detected in the property cache, probably as a result of hardware failure or abrupt shutdown. The error was fixed.
Very low disk space was detected on drive <*drive*>. Please free up at least <*number*> MB of space for content index to continue.	Free space has fallen below the minimum threshold. No merges or filtering will take place until some disk space is freed up.
Added virtual root <root> to index.	The message Mapped to <path> is added when a virtual root is indexed.
Removed virtual root <root> from index.	This message is added when a virtual root is deleted from the index.
Added scope <path> to index.	This message is added when a new physical scope is indexed.
Removed scope <path> from index.	This message is added when a new physical scope is deleted from the index.

* Compiled from the IIS 4.0 help file ixerrlog.htm.

Modifying Index Server Registry Keys

Many of the errors listed in the previous tables can be addressed by modifying the Registry. For example, when you see the message "The query failed because the Web server is busy processing other requests," you can allow more queries to be added to the queue by increasing the value of the IsapiRequestQueueSize Registry key. Table 7.7 lists Registry keys that pertain to Index Server operations.

Table 7.7 *Index Server Parameters in the Registry*

Parameter	Description
DaemonResponseTimeout	Timeout value to determine if the CiDaemon process is looping because of a corrupted file. Measured in minutes. Range is 1 to 120. Default is 5.
EventLogFlags	Controls the generation of event log messages. Measured as a Bit-Field. Range is 0 to 7. Default is 0x00000002.
FilterContents	If set to 0, contents of files will not be filtered. Only properties are filtered. When set to a nonzero value, contents and properties will be filtered. Measured as a Boolean. Range is 0 and 1. Default is 1.
FilterDirectories	When set to a nonzero value, directories will also be filtered for system properties and displayed in query results. Measured as a Boolean. Range is 0 and 1. Default is 0.
FilterFilesWithUnkownExtensions	Determines if files with extensions that have not been registered will be filtered or not. Set the value to 0 if only registered file types should be filtered. To see how to register a file type, see Associating File Types with Extensions on the "Filtering" page. Measured as a Boolean. Range is 0 and 1. Default is 1.
FilterRetries	The maximum number of times a file will be retried for filtering if there are failures while trying to filter a file. Measured in number. Range is 1 to 10. Default is 4.
FilterRetryInterval	The number of seconds between attempts to filter the contents of a file that is being used by another process. Measured in number. Range is 2 to 240. Default is 30 seconds.
ForcedNetPathScanInterval	Time interval between forced scans on directories with no notifications. Measured in minutes. Range is 10 to infinity. Default is 120.
GenerateCharacterization	Controls automatic generation of characterization (abstract). Measured as a Boolean. Range is 0 and 1. Default is 1.
GrovelIISRegistry	Controls whether all virtual roots are automatically indexed or not. Measured as a Boolean. Range is 0 and 1. Default is 1.

Table 7.7, continued.

Parameter	Description
IsapiMaxEntriesInQueryCache	Maximum number of the cached queries. Range is 5 to 100. Default is 10.
IsapiMaxRecordsInResultSet	Maximum total number of rows to fetch for a single query. Range is -1000000. Default is 5000.
IsapiMaxRecordsPerGetRows	Maximum number of rows to fetch when getting data to display on an HTML page. Range is 10 to 1000. Default is 50.
IsapiQueryCachePurgeInterval	Time interval a query cache item will remain alive. Measured in minutes. Range is 1 to 120. Default is 5.
IsapiRequestQueueSize	Maximum number of Web query requests to queue when busy with other queries. Range is -100000. Default is 16.
IsapiRequestThresholdFactor	Number of threads per processor beyond which query requests are queued. Range is 1 to 100,000. Default is 3.
MasterMergeCheckpointInterval	Checkpointing interval for master merge. Determines how much work (data written to the new master index) to redo in case a master merge is paused and restarted. Measured in Kilobytes. Range is 512 to 8096. Default is 512.
MasterMergeTime	Time at which master merge will occur. This is stored as the number of minutes after midnight. Measured in minutes. Range is 0 to 1439. Default is 0.
MaxActiveQueryThreads	Maximum number of query threads. This establishes the maximum number of concurrently processed asynchronous queries. Measured in threads. Range is 1 to 1000. Default is 2.
MaxCharacterization	Number of characters in the automatically generated characterization (abstract). Measured in characters. Range is 20 to 500. Default is 320.
MaxFilesizeFiltered	Maximum size of a single file to be filtered using the default filter. If the default filter is used for a file bigger than this number, only properties will be filtered. Note that this limit does not apply for registered file types. Measured in Kilobytes. Range is 0 to infinity. Default is 256.
MaxFilesizeMultiplier	Maximum amount of data that can be generated from a single file, based on its size. This value is a multiplier. A value of 3 means that a file can generate up to three times its size in content index data. Measured in number. Range is 4 to 0xFFFFFFFF. Default is 8.
MaxFreshCount	Maximum number of files whose latest indexed data is not in the master index. When this limit is reached, a master merge will start. Measured in documents. Range is 1000 to 40,000. Default is 5000.

Table 7.7, continued.

Parameter	Description
MaxIdealIndexes	Maximum number of indexes considered acceptable in a well-tuned system. When the number of indexes climbs above this number and the system is idle, an annealing merge will take place to bring the total count of indexes to this number. Measured in indexes. Range is 2 to 100. Default is 5.
MaxIndexes	Maximum number of persistent indexes in the catalog. If this number is exceeded, a shadow merge will be performed to bring the total below this number. Measured in indexes. Range is 10 to 150. Default is 50.
MaxMergeInterval	Sleep time between merges. Index Server activates this often to determine if a merge is necessary. This is usually an annealing merge but may be a shadow or master merge. Measured in minutes. Range is 1 to 60. Default is 10.
MaxPendingDocuments	The number of pending documents to be filtered before considering CI out-of-date for property queries. Measured in documents. Range is 1 to 50,000. Default is 32.
MaxQueryExecutionTime	Maximum execution time of a query. If a query takes more than this amount of CPU time, processing of it will be stopped and an error status will be indicated. Measured in milliseconds of CPU time. Range is 50 to infinity. Default is 10,000.
MaxQueryTimeslice	Maximum amount of time to execute a single query in a timeslice. If more asynchronous queries are active than allowed query threads, a query is put back on the pending queue after this time interval. Time slicing is done after a matching row is found, so the time spent in a timeslice may overrun this and a considerable number of rows may be examined in the timeslice. Measured in milliseconds of CPU time. Range is 1 to 1000. Default is 50.
MaxQueueChunks	Maximum number of in-memory buffers for keeping track of pending documents. The higher the number, the less frequently it has to be written to disk. Measured in number of chunks. Range is 10 to 30. Default is 20.
MaxRestrictionNodes	If query normalization creates a query restriction greater than the number of nodes set in this Registry entry, the query fails with the status of QUERY_E_TOO COMPLEX. This status message means the limit imposed in this Registry key has been reached. This key keeps a user from overloading the server's capacity with an overly large query. Measured in number of nodes. Range is 1 to 4 billion. Default is 250.

Table 7.7, continued.

Parameter	Description
MaxShadowFreeForceMerge	On the catalog drive, if the free space falls below MinDiskFreeForceMerge and the disk space occupied by the shadow indexes exceeds MaxShadowFreeForceMerge, a master merge is started. This is measured in percentage of disk space. Range is 5 to 25. Default is 15.
MaxShadowIndexSize	If the disk space occupied by the shadow indexes exceed this percentage of the catalog drive, a master merge is stated. Measured in percentage of disk space. Range is 5 to infinity. Default is 20.
MaxWordLists	Maximum number of word lists that can exist at one time. Measured in WordLists. Range is 10 to 30. Default is 20.
MaxWordlistSize	Maximum amount of memory taken up by an individual word list. When this limit is reached, only the document being filtered will be added. Additional documents will be re-filed and placed later in another word list. Measured in 128 Kbyte units. Range is 10 to infinity. Default is 14.
MinDiskFreeForceMerge	On the catalog drive, if the free space falls below MinDiskFreeForceMerge and the disk space occupied by the shadow indexes exceeds MaxShadowFreeForceMerge, a master merge is started. This is measured in percentage of disk space. Range is 5 to 25. Default is 15.
MinIdleQueryThreads	Minimum number of idle threads kept alive to process incoming queries. Range is 0 to 1000. Default is 1.
MinMergeIdleTime	If average system idle time for the last merge check period is greater than this value, an annealing merge can be performed. Measured in percentage of CPU. Range is 10 to 100. Default is 90.
MinSizeMergeWordlists	Minimum combined size of word lists that will force a shadow merge. This is measured in Kilobytes. Range is 1024 to 10240. Default is 1024.
MinWordlistMemory	Minimum free memory for word list creation. Measured in Megabytes. Range is 1 to 10. Default is 5.
PropertyStoreMappedCache	Maximum size of in-memory buffers for Property Cache. Measured in 64 Kbyte pages. Range is 0 to infinity. Default is 16.
ThreadClassFilter	Priority class of the CiDaemon process. The value 20 is Normal Priority Class, 40 is Idle Priority Class, 80 is High Priority Class, and 100 is Realtime Priority Class. Measured in Idle Priority Class. Range is 20, 40, 80, and 100. No default value.
ThreadPriorityFilter	Priority of the filtering thread within the CiDaemon process. Measured as 'above normal'. Default is 'lowest to above normal'.
ThreadPriorityMerge	Priority of the merge thread. Measured as 'normal'. Default is 'lowest to above normal'.

Study Break

Study Break: Monitoring Event Viewer

Practice what you have learned by viewing the application event log. To do this, launch the Event Viewer application from the Administrative Tools program group. Next, select Application from the File menu. Double-click on items relating to the Index Server to view the error messages.

MCSE 7.5 Troubleshooting Installations

In this section, you will learn some of the ways you can go about troubleshooting setup and installation problems.

As previously described, you should remove previous versions of IIS and disable other Web, FTP, or Gopher services running on your server before installing IIS 4.0. In addition, you must have Windows NT Server 4.0, Service Pack 3 (or later), and Internet Explorer 4.01 (or later) installed. In most cases, installation and setup will be trouble-free. When it is not, there are several sources to which you may turn for help.

Online Help

To open the Help dialog box, as shown in Figure 7.48, select the Help command from the Start menu.

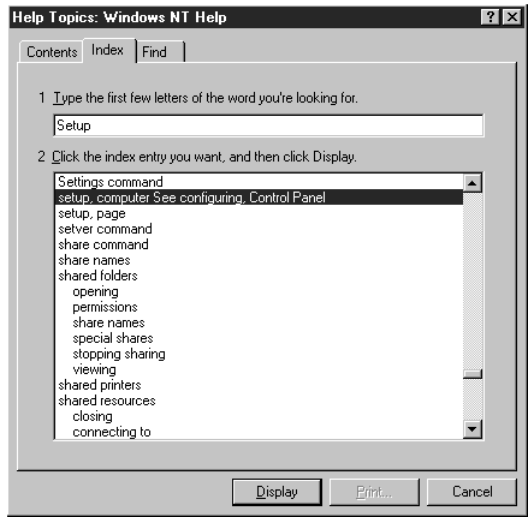

Figure 7.48 *Viewing Windows NT Server's Online Help Topics Dialog Box.*

The IIS also provides online help. To view it, select Product Documentation from the Programs menu.

Web Sites

Microsoft provides Web sites that support both Windows NT Server and the IIS. One of the most useful, TechNet, provides a troubleshooting database, as shown in Figure 7.49.

At these sites you can find bug fixes, software updates, and technical notes on known problems and software incompatibilities. Useful Web sites include the following:

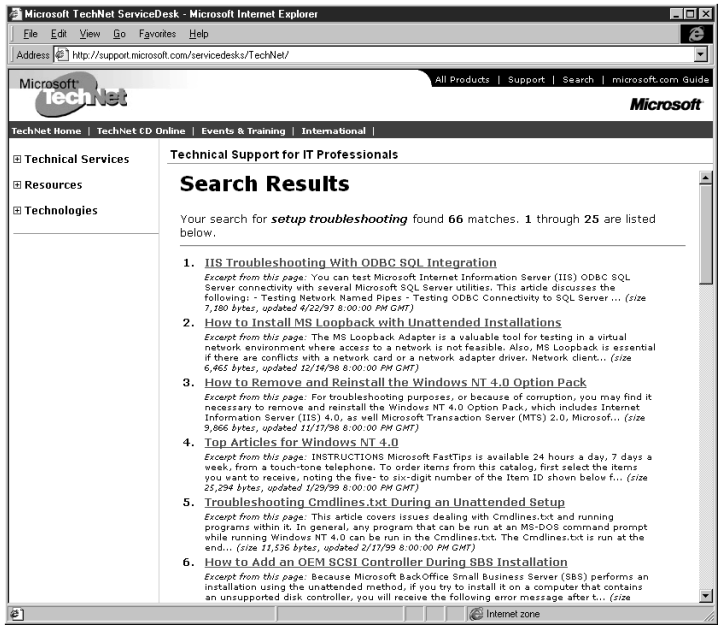

Figure 7.49 *Viewing the Microsoft Troubleshooting Database Web Site.*

- The Microsoft Support site is located on the WWW at http://www.microsoft.com/support.
- The Microsoft Personal Support site is located on the WWW at http://support.microsoft.com/support.
- The Microsoft TechNet site is located on the WWW at http://support.microsoft.com/servicedesks/TechNet.
- The Microsoft Windows NT Server support site is located on the WWW at http://www.microsoft.com/ntserver.
- The Microsoft IIS support site is located on the WWW at http://www.microsoft.com/ntserver/Web

Microsoft TechNet

The Microsoft TechNet program, available through Microsoft sales, provides subscribers with service packs, drivers, updates, and technical information on CD-ROM, as shown in Figure 7.50.

Subscribers are sent updated TechNet CD-ROMs monthly.

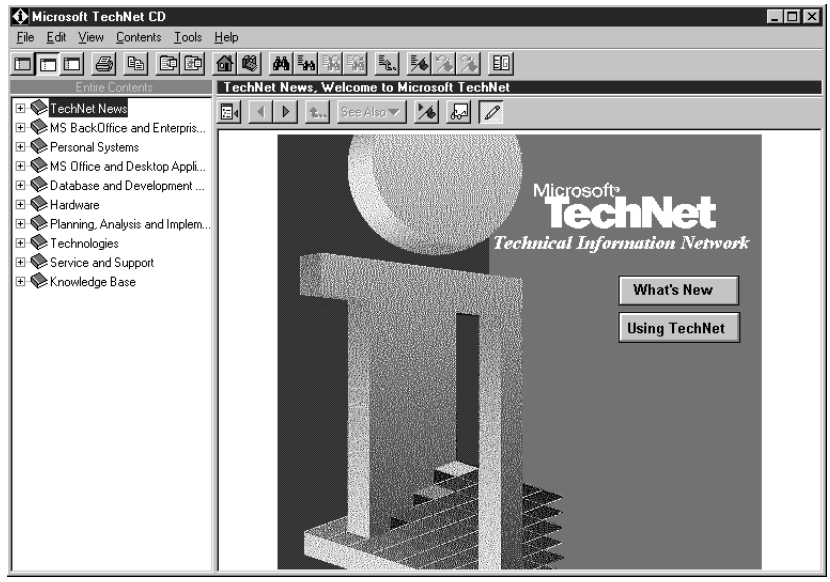

Figure 7.50 *Viewing the TechNet CD-ROM.*

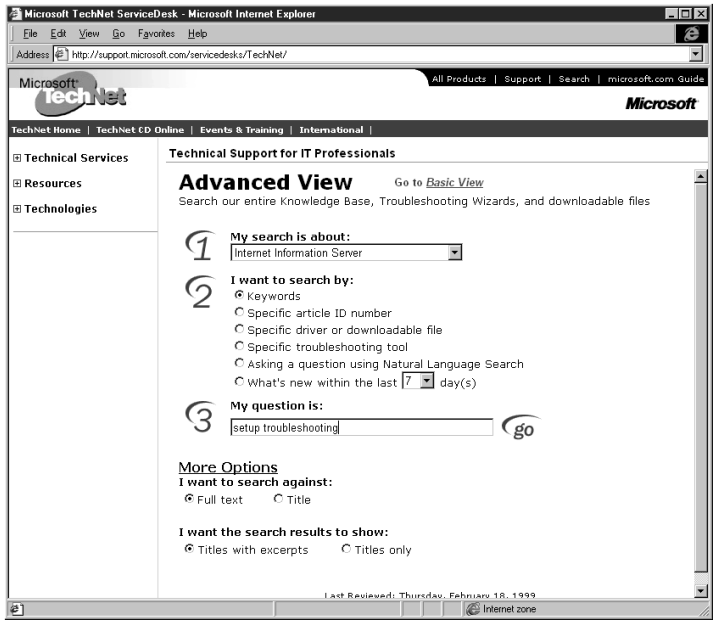

Figure 7.51 *Searching for Troubleshooting Information.*

Study Break

Study Break: Look Up Tech Notes

Practice what you have learned by visiting the TechNet site and using the troubleshooting database.

Use the Web site's search engine (see Figure 7.51) to look for information relating to IIS 4.0 setup issues, or information about any other IIS-related problems that you might be having.

MCSE 7.6 Repairing Broken Links

In this section, you will learn to use Content Analyzer's WebMaps to find and fix broken links, as well as identify other Web site problems.

As previously described, you can use Site Server Express' Content Analyzer to create WebMaps, graphical representations of your Web site's structure, as shown in Figure 7.52. Once created, you can analyze the WebMap to locate errors in your Web site's design.

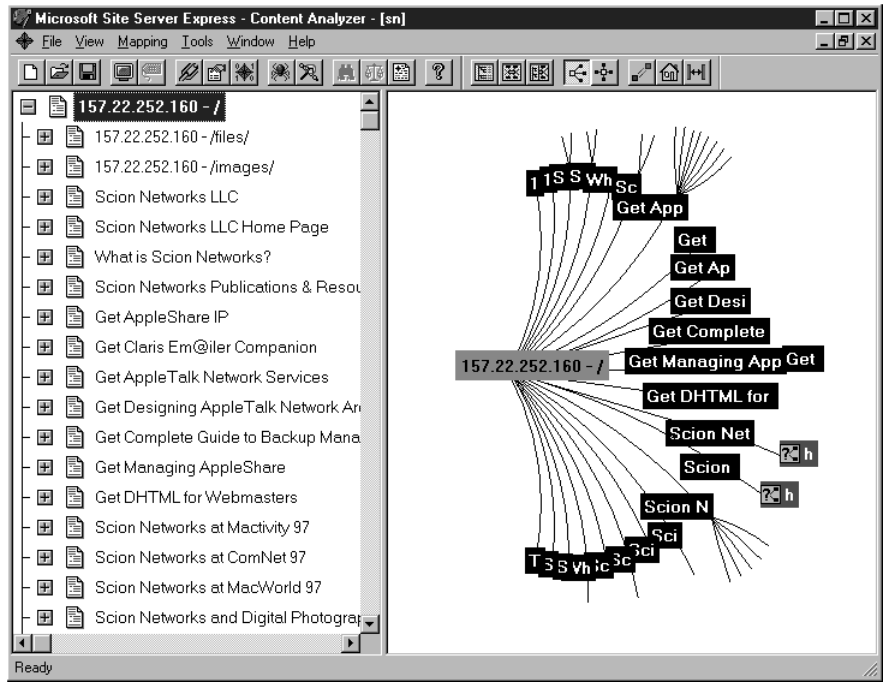

Figure 7.52 *Viewing a WebMap.*

To view your site's link information, click on the Object Links toolbar button to open the Link Info window, as shown in Figure 7.53.

By selecting the Links on Page radio button, you can view all of the hyperlinks present on a given page.

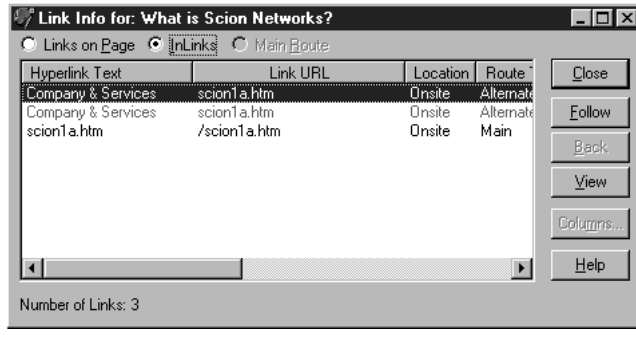

Figure 7.53 *Viewing the Link Info Window's Links on Page.*

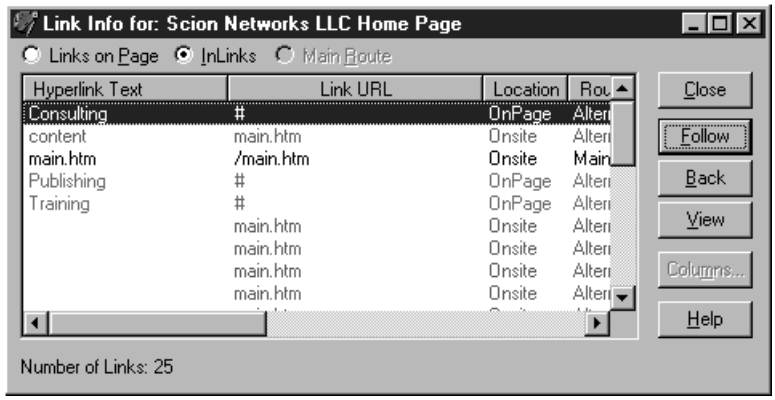

Figure 7.54 *Viewing the Link Info Window's InLinks.*

By selecting the InLinks radio button, you can view links that reference the page you are viewing, as shown in Figure 7.54. These can be local to the Web site or on other sites.

Using Quick Search

Once you have created a WebMap you can then use Content Analyzer's Quick Search command, launched from the Tools menu or the menu bar, to hunt for various problems.

BROKEN LINKS

Use the Broken Links command in the Quick Search fly-out menu under the Tools menu to search for links that do not connect to valid resources, as shown in Figure 7.55.

To correct a broken link, select the page and choose the Launch Helper App command from the Tools menu to open an HTML editor application.

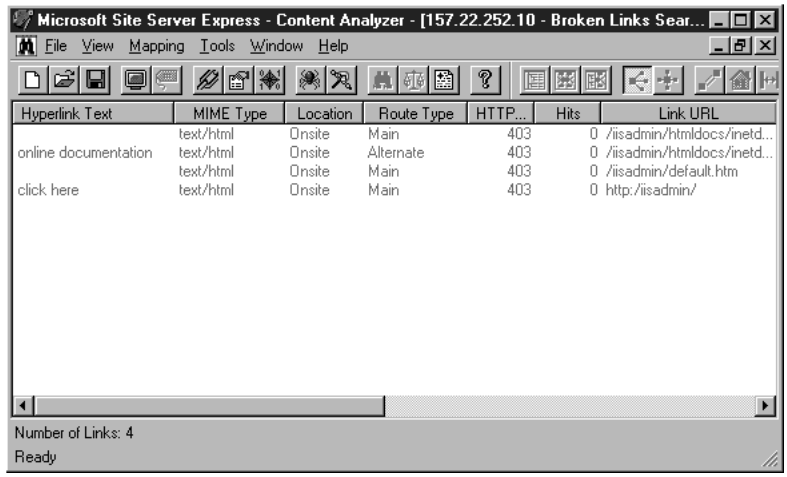

Figure 7.55 *Finding Broken Links with the Quick Search Command.*

HOME SITE OBJECTS

Use the Home Site Objects command in the Quick Search fly-out menu under the Tools menu to search for all home site objects (see Figure 7.56).

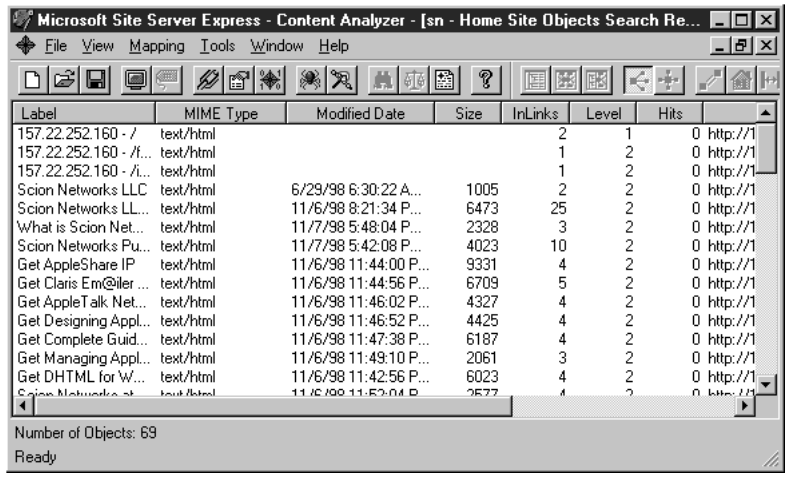

Figure 7.56 *Finding Home Site Objects with the Quick Search Command.*

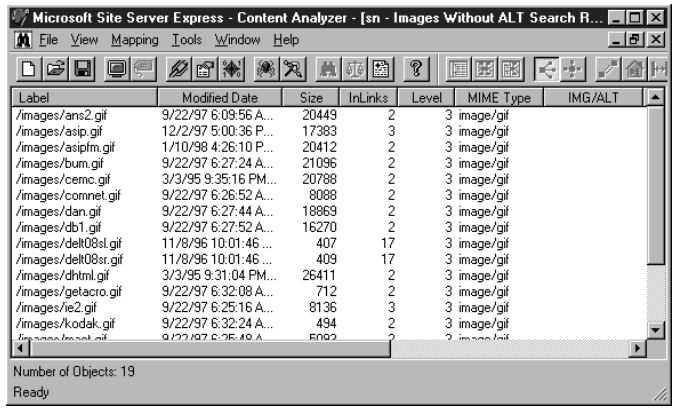

Figure 7.57 *Finding Images without ALT Tags Using the Quick Search Command.*

IMAGES WITHOUT ALT

Use the Images Without ALT command in the Quick Search fly-out menu under the Tools menu to search for all images that are not associated with an ALT tag, as shown in Figure 7.57.

LOAD SIZE OVER 32K

Use the Load Size Over 32K command in the Quick Search fly-out menu under the Tools menu to search for objects that are larger than is optimal for fast downloading, as shown in Figure 7.58.

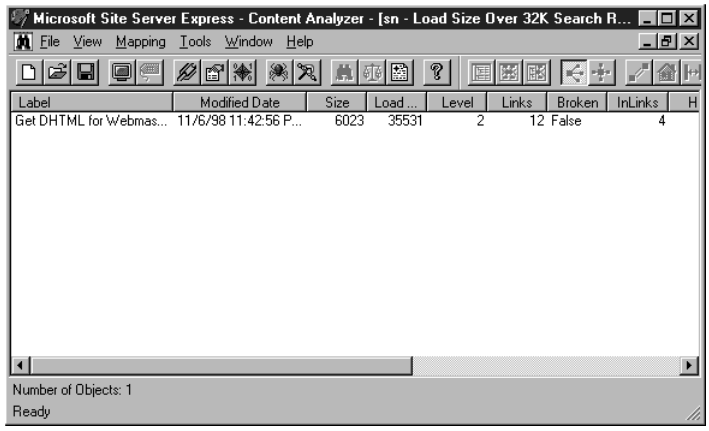

Figure 7.58 *Finding Objects over 32 Kbytes with the Quick Search Command.*

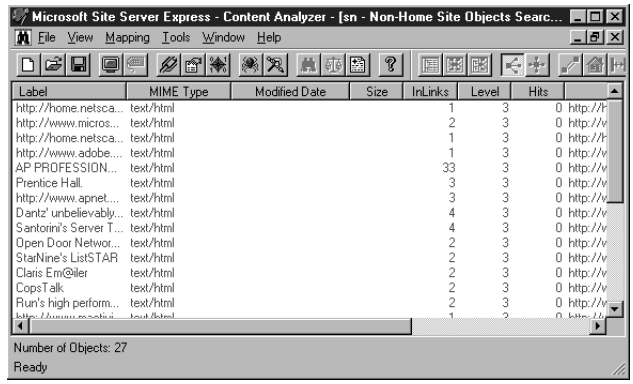

Figure 7.59 *Finding Non-Home Site Objects with the Quick Search Command.*

NON-HOME SITE OBJECTS

Use the Non-Home Site Objects command in the Quick Search fly-out menu under the Tools menu to search for objects not located at the home site, as shown in Figure 7.59.

NOT FOUND OBJECTS

Use the Not Found Objects command in the Quick Search fly-out menu under the Tools menu to search for objects that cannot be found and which generate the 404 error, as shown in Figure 7.60.

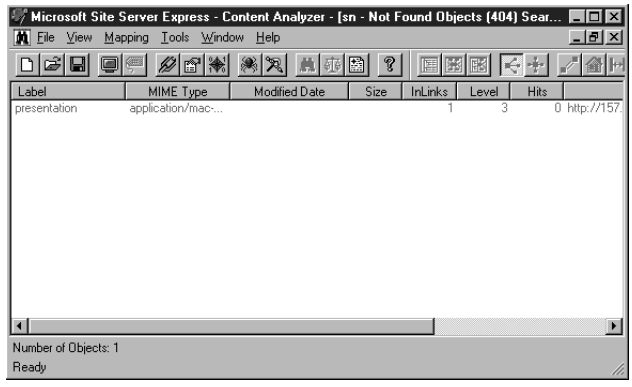

Figure 7.60 *Identifying Not Found Objects with the Quick Search Command.*

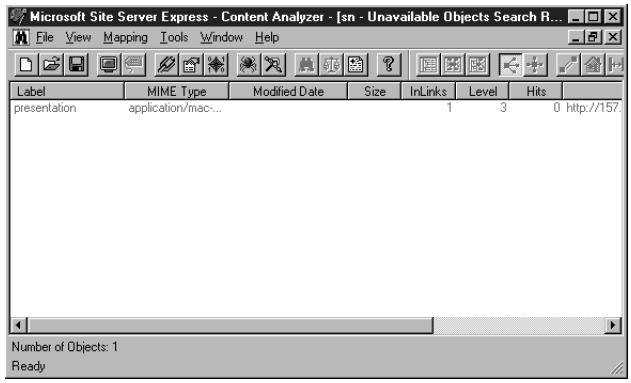

Figure 7.61 *Identifying Unavailable Objects with the Quick Search Command.*

UNAVAILABLE OBJECTS

Use the Unavailable Objects command in the Quick Search fly-out menu under the Tools menu to search for objects that cannot be accessed, as shown in Figure 7.61.

UNVERIFIED OBJECTS

Use the Unverified Objects command in the Quick Search fly-out menu under the Tools menu to search for objects that have not been checked, as shown in Figure 7.62.

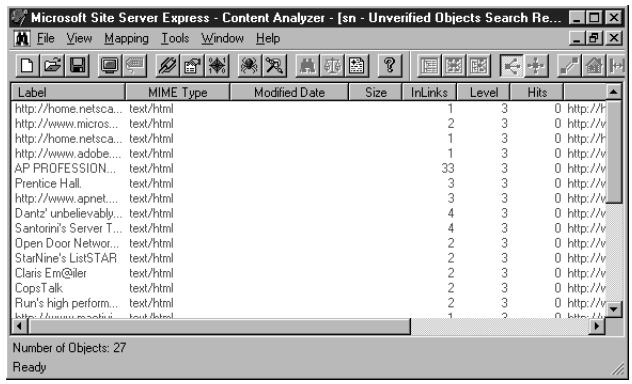

Figure 7.62 *Identifying Unverified Objects with the Quick Search Command.*

Study Break

Study Break: Check for Broken Links

Practice what you have learned by searching for broken links. First, create a WebMap of your site. Next, use either the Quick Search or Custom Search command to locate broken links. Use the Launch Helper App command to open an HTML editor application in which to correct the links.

MCSE 7.7 Troubleshooting WWW Services

In this section, you will learn to troubleshoot problems with the IIS WWW Service.

As previously described, Web browsers expect to find Web services running at port 80. If Web browsers are having trouble connecting, make sure that you have either left the default configuration of port 80 or that you have told your users what the new port number is. You can use port numbers above 1024, but if you do so users will need to add the new port to the URL in the following format:

```
http://<host_name>:<port>
```

By default, the Web server is configured to launch at server bootup. It can be stopped or paused from the Internet Service Manager application, however, or disabled in the Services Control Panel application. Another thing to check when users cannot connect, then, is that someone has not turned the server off.

Yet another issue can arise if users are not granted at least Read permissions to the Web site directory. Also, if you are extending anonymous access, check to make sure that the IUSR account has not been disabled.

Finally, a number of other WWW Service problems are reported by HTTP error codes, as listed in Table 7.8.

Table 7.8 *Common HTTP Error Codes*

Code	Parameter	Description
151	DNS Hostname Lookup Failure	The DNS server cannot resolve an IP address that is associated with the URL requested.
152	Unable To Connect	DNS could resolve the address, but the Web browser could not connect to the Web server.
153	Incomplete HTTP Header Response	The Web page that is queried usually returns the full HTTP header in the first packet sent back. This code often shows up with a specific Web server: N.E.T. 1.0.
OK	The Web page is accessible.	
401	Password Protected	The Web browser does not have permission to search through protected areas of the Web site.
403	Forbidden	The request for object access was denied. This can happen when a Web server is busy.
404	File Not Found	The Web server is available, but the Web page is not accessible.
500	Internal Server Error	The Web server is probably down.

Study Break

Study Break: Search for Errors

Practice what you have learned by searching for error messages, such as those listed in Table 7.8, that are generated by your Web site.

One way to do this is to use a Web browser to check every link. While this is time consuming, it also gives you a chance to check the presentation effect of each Web page. An easier method is to use Content Analyzer to query the Web server, as previously described. If any of these error messages are encountered, troubleshoot the cause.

MCSE 7.8 Troubleshooting FTP Services

In this section, you will learn to troubleshoot problems with the IIS FTP Service.

As previously described, FTP clients expect to find FTP services running at port 21. If users are having trouble connecting, make sure that you have either left the default configuration of port 21 or that you have told your users what the new port number is. You can use port numbers above

1024, but if you do so users will need to add the new port to the URL in their Web browsers in the following format:

```
ftp://<host_name>:<port>
```

By default, the FTP server is configured to launch at server bootup. It can be stopped or paused from the Internet Service Manager application, however, or disabled in the Services Control Panel application. When users cannot connect, make sure the service has not been turned off.

Another issue can arise if users are not granted sufficient permissions to the FTP site directory. If it is a download-only site, then Read permissions should be enabled. If it is an upload site as well, be sure to enable Change permissions.

If you are extending anonymous access, check to make sure that the IUSR account has not been disabled and that the Allow Anonymous Access checkbox has been enabled in the Properties dialog box of each site (as previously described).

You can test FTP connectivity under Windows NT by launching the FTP client from the Command Prompt. Its options are as follows:

- -v Suppress display of remote server responses.
- -n Suppress auto-logon on initial connection.
- -i Turn off interactive prompts on multiple transfers.
- -d Enable debugging.
- -g Disable file name globbing.
- -s:<file_name> Launch file containing scripted FTP commands.
- -a Use any local interface when binding data connection.
- -w:<buffersize> Override default buffer size of 4096.
- host Specify server by host name or IP address.

Study Break

Study Break: Transfer Files with FTP

Practice what you have learned by moving files to and from your FTP site with an FTP client, such as the one included in Windows NT.

Use the "FTP?" command at the Command Prompt to view options. Use the Open command in command interpreter mode to specify the remote host. Use the Get command to download a file from the site. Use the Put command to upload a file to the site. Use the Close command to close the connection. If there are problems, use the Debug command to help diagnose them.

■ Summary

This chapter examined some of the issues surrounding troubleshooting IIS problems, including those relating to configuration and setup, security, resource access, Index Server queries, broken hyperlinks, the WWW Service, and the FTP Service.

Troubleshooting Configurations

The IIS runs under Windows NT Server 4.0 on either an Intel- or RISC-based computer. Windows NT Server and IIS 4.0 will run on as modest a machine as a 90 MHz. 486DX with 32 Mbytes or RAM. At least a 150 MHz. processor and 48 Mbytes of RAM is required for a RISC-based computer. In addition to Windows NT Server 4.0, the Windows NT Option Pack 4.0 requires the latest Service Pack (version 3 or later).

The Event Viewer application can be used to identify services that fail to launch on the Windows NT Server at startup, along with other data. Windows NT Diagnostics provides detailed system configuration information. The Recovery utility can be used to log debugging information.

Networking configuration is performed through the Network Control Panel application. Here you can configure such variables as computer identification, network services, adapters and bindings, and protocols. In configuring TCP/IP, you should pay particular attention to the IP address, subnet mask, gateway address, and DNS settings. TCP/IP errors most commonly involve the misconfiguration of these settings.

Troubleshooting Security

In troubleshooting security, one is either attempting to keep people from getting access to resources that they should be restricted from, or to give people access to resources they should have. Common problems in this area involve firewalls, anonymous access, user logons, network access, port numbers, NTFS permissions, and SSL connections and server certificates.

Troubleshooting Resource Access

When users have trouble accessing a networked resource, protocol misconfiguration is commonly to blame. You can use the IPCONFIG or WINIPCFG utility to identify the TCP/IP configuration of a host computer. You can use the PING utility to test network connectivity. With PING you should verify the local host with a loopback address, a host on the same subnet, the gateway router, and a host on a remote subnet or the Internet. You can use the

TRACERT utility to follow the path of packets through gateways between the local and remote hosts. You can use the NETSTAT utility to see the TCP sessions running on the host. You can use the HOSTNAME and NBSTAT utilities to troubleshoot name resolution problems. Name resolution problems commonly involve severed network access, incorrectly configured DNS or WINS servers, or improperly written HOSTS and LMHOSTS files.

Troubleshooting Index Server Queries

Common problems affecting Index Server operations are query errors and .idq file errors. Indexing and cataloging errors can be detected by monitoring the Windows NT application log. Many of the parameters affecting these operations can be changed in the Registry.

Troubleshooting Installations

You should remove previous versions of IIS and disable other Web, FTP, or Gopher services running on your server before installing IIS 4.0. In addition, you must have Windows NT Server 4.0, Service Pack 3 (or later), and Internet Explorer 4.01 (or later) installed. In most cases, installation and setup will be trouble-free. When it is not, there are several sources that you can look to for help, such as online help, Microsoft's Web sites, and the TechNet program.

Repairing Broken Links

After creating a WebMap using the Site Server Express Content Analyzer application, you can track down broken links and other problems with the Quick Search or Custom Search command. You can launch a helper application, such as an HTML editor, to correct these problems.

Troubleshooting WWW Services

Web browsers expect to find Web services running at port 80. If Web browsers are having trouble connecting, make sure that you have either left the default configuration of port 80 or that you have told your users what the new port number is. The Web server is configured to launch at server bootup. It can be stopped or paused from the Internet Service Manager application, however, or disabled in the Services Control Panel application. This is another thing to check when users are unable to connect. Another

issue can arise if users are not granted at least Read permissions to the Web site directory.

Troubleshooting FTP Services

FTP clients expect to find FTP services running at port 21. If users are having trouble connecting, make sure that you have either left the default configuration of port 21 or that you have told your users what the new port number is. The FTP server is configured to launch at server bootup. It can be stopped or paused from the Internet Service Manager application or disabled in the Services Control Panel application, however. Another issue can arise if users are not granted sufficient permissions to the FTP site directory. If it is a download-only site, then Read permissions should be enabled. If it is an upload site as well, be sure to enable Change permissions. If you are extending anonymous access, check to make sure that the IUSR account has not been disabled and that the Allow Anonymous Access checkbox has been enabled in the Properties dialog box of each site.

▲ Chapter Review Questions

Here are a few questions relating to the material covered in the *Troubleshooting* section of Microsoft's *Implementing and Supporting Microsoft Internet Information Server 4.0* exam (70-087).

1. *Which of the following are required for installation of the IIS 4.0? Choose all that apply.*

   A. Windows NT Option Pack 4.0

   B. Windows NT Service Pack 2

   C. Internet Explorer 2.0

   D. Windows NT Server 4.0

2. *Which of the following are TCP/IP settings that are commonly misconfigured on network clients? Choose all that apply.*

   A. Static IP address

   B. Subnet mask

   C. Computer name

   D. Default gateway

3. *If the IUSR account is disabled, no users will be able to gain access to Web or FTP resources.*

   A. True

   B. False

4. *Under SSL, secure connections can be created between the server and client using a private key encryption scheme.*

   A. True

   B. False

5. *If you want to know which settings a DHCP server has leased to a client computer, you may type the IPCONFIG /all command at the command prompt.*

   A. True

   B. False

6. *Which of the following are procedures useful in troubleshooting with the PING utility? Choose all that apply.*

   A. Ping the local host

   B. Ping a remote host on the same subnet

   C. Ping the default gateway router

   D. Ping a remote host on a another subnet

7. *The way in which the Index Server indexes words for importance is referred to as word weighting.*

   A. True

   B. False

8. *The application log registers errors under the CiErrorMessages category.*

   A. True

   B. False

9. *You should make sure all existing Web, Gopher, and FTP services are running before you install the Windows NT 4.0 Option Pack.*

   A. True

   B. False

10. *You can locate broken Web site links and a number of other errors using Internet Service Manager.*

    A. True

    B. False

11. *Broken links can only be detected for Web pages on the local server.*

A. True

B. False

12. *If you wish to hide your Web site, you can change its default port number to anything above 80.*

A. True

B. False

13. *HTTP error code 404 refers to a failure in DNS name resolution.*

A. True

B. False

14. *To be able to upload and download files from an FTP directory, users must have at least Read permissions.*

A. True

B. False

15. *Get is an FTP command that can be used to download files, while Put is an FTP command that can be used to upload files.*

A. True

B. False